Simulation von Privatsphärenschutz in Fahrzeug-Ad-hoc-Netzen[1]

David Eckhoff[2]

Abstract: Der drahtlose Datenaustausch zwischen Fahrzeugen ist eine vielversprechende Technologie, um die Sicherheit im Straßenverkehr zu erhöhen. Gleichzeitig könnte die große Menge an erhobenen und gesendeten Daten jedoch starke Einschnitte in die Privatsphäre der Fahrer bedeuten. Die diesem Artikel zugrunde liegende Dissertation beschäftigt sich mit der simulativen Bewertung von Privatsphäre in Fahrzeug-Ad-hoc-Netzen. Die vorgestellte Methodik ermöglichte es, das Privatsphärenproblem detailliert zu erfassen und darauf aufbauend umsetzbare und vor allem zu Sicherheitsfunktionen kompatible Vorschläge auszuarbeiten und zu bewerten.

1 Einführung

Moderne Kraftfahrzeuge bestehen aus einer Vielzahl an Steuergeräten, d.h. kleinen Computern mit spezifischen Aufgaben, wie z.B. der Regelung des Blinkers oder das Auslösen des Airbags im richtigen Moment. Viele Aktionen im Fahrzeug werden von mehreren Steuergeräten gleichzeitig und in Kooperation ausgeführt, was wiederum erfordert, dass diese Computer die Möglichkeit haben miteinander zu kommunizieren. Bei über 100 Steuergeräten pro Fahrzeug, gekoppelt über diverse Bussysteme, kann man sagen, dass Fahrzeuge heutzutage mobile Computernetzwerke sind. Der nächste logische Schritt ist es demnach, Fahrzeuge auch untereinander zu verbinden und in Form von drahtloser Kommunikation Datenaustausch zu ermöglichen.

Die Hauptmotivation dieser Car-2-Car-Systeme ist vor allem die Steigerung der Verkehrssicherheit. Fahrzeuge senden periodisch (z.B. mit einer Frequenz von 10 Hertz) über ein WLAN-System unter anderem ihre Position und Geschwindigkeit; Fahrzeuge in Reichweite (typischerweise bis ca. 500 Meter) empfangen diese Nachrichten und können sich dadurch eine virtuelle Umgebung aufbauen. So wird die frühzeitige Erkennung von Gefahrensituationen ermöglicht, um entweder den Fahrer zu warnen oder automatisierte Eingriffe in die Fahrzeugdynamik vorzunehmen. Die Standardisierung dieser Systeme in Europa (ETSI ITS-G5) und den USA (IEEE WAVE) ist bereits fortgeschritten und zudem haben diverse Feldtests weltweit gezeigt, dass die Technologie ausgereift genug ist. Aus technischer Sicht stünde einer Einführung demnach nichts im Wege.

Die oftmals vernachlässigte Schattenseite solcher allgegenwärtiger Systeme ist die Gefährdung der Privatsphäre des Fahrers. Das periodische und unverschlüsselte Senden von Statusinformationen in Car-2-Car-, oder allgemeiner, Car-2-X-Systemen, könnte dazu miss-

[1] Englischer Titel der Dissertation: “Simulation of Privacy-Enhancing Technologies in Vehicular Ad-Hoc Networks”

[2] Friedrich-Alexander-Universität Erlangen-Nürnberg, david.eckhoff@fau.de

braucht werden, Fahrer virtuell zu verfolgen, d.h. zu jeder Zeit Informationen über den Aufenthaltsort einer Person zu erhalten. Der gravierende Unterschied zu Mobiltelefonen ist, dass der Fahrer in der Regel keine Wahl hat das Gerät abzuschalten, weil ein Betrieb entweder vom Gesetzgeber vorgeschrieben ist, oder, wenn ein Abschalten möglich wäre, der Fahrer gezwungen würde sich zwischen Sicherheit und Privatsphäre zu entscheiden. Ein weiterer Aspekt ist, dass diese Systeme ununterbrochen Informationen übermitteln, d.h. auch wenn ein Fahrer zu schnell fährt oder z.B. einen Spurwechsel ohne Blinken durchführt. Diese Daten können sicherlich helfen, um im Falle eines Unfalles die Schuldfrage zu klären. Jedoch können sie auch missbraucht werden, um ein vollautomatisiertes Verkehrsüberwachungssystem zu installieren, in dem jeder Fahrer bei der kleinsten Ordnungswidrigkeit mit einer Geldstrafe belegt wird. Diese Art von allgegenwärtiger Überwachung hat den Beigeschmack einer Orwellschen Dystopie, die, wenn auch zu diesem Zeitpunkt etwas schwarz-malerisch, einen entscheidenden Einfluss auf das Freiheitsgefühl der Bürger haben würde. Neue Technologien und Systeme sollten also so konzipiert werden, dass sie einen solchen Missbrauch nicht ermöglichen, aber dennoch ihren Zweck vollständig erfüllen können.

Die größte Problematik bei der Evaluierung, ob ein System die Anforderungen an den Privatsphärenschutz erfüllt, ist dass Privatsphäre selber ein unscharfer Begriff ist, der schwer zu isolieren und noch schwerer zu quantifizieren ist. Genau dies ist aber notwendig um beurteilen zu können, ob eine Variante des Systems die Privatsphäre mehr schützt als eine andere. Die diesem Artikel zugrunde liegende Dissertation beschäftigt sich genau mit dieser Fragestellung, nämlich wie komplexe Systeme wie Fahrzeugnetze simuliert werden können, um Erkenntnisse über die Gefährdung der Privatsphäre zu erlangen. Darauf basierend werden eigene Methoden zum Privatsphärenschutz vorgestellt und analysiert.

2 Privatsphäre in Fahrzeugnetzen

Um überhaupt Privatsphärenschutz zu ermöglichen, muss der Begriff Privatsphäre zuerst definiert werden. Alan Westin definiert ihn als „die Fähigkeit eines Individuums die Rahmenbedingungen, unter welchen persönliche Informationen gesammelt und benutzt werden, zu bestimmen" [We67]. Persönliche Informationen werden von der EU als „jegliche Informationen die eine [...] identifizierbare Person betreffen" [Eu95] definiert. Nissenbaum spezifiziert etwas schärfer und definiert Privatsphäre im Rahmen von kontextabhängiger Integrität [Ni04], d.h. jeglicher persönlichen Information hängt ein Kontext an (z.B. ein Arztbesuch) wobei ein Verwenden außerhalb dieses Kontextes eine Verletzung der Privatsphäre darstellt. Solch ein Eingriff in die Privatsphäre kann weitreichende Konsequenzen haben, wie z.B. aufdringliche Werbung, Veröffentlichung von Informationen, die zu Unannehmlichkeiten oder Demütigung der betroffenen Person führen, bis hin zum Missbrauch durch totalitäre Regierungen, die im schlimmsten Fall sensible Informationen (wie z.B. den Aufenthaltsort) benutzen, um politische oder soziale Minderheiten zu verfolgen [SHG03].

Privatsphäre kann in verschiedene Teilbereiche untergliedert werden, z.B. nach Finn et. al [FWF13], die unter anderem zwischen Privatheit der Person, des Verhaltens und des

Ortes unterscheiden. Zusätzlich zu diesen Teilbereichen definieren Pfitzmann und Hansen [PH10] verschiedene Aspekte von Privatsphäre, die durch technische Methoden geschützt werden können. Diese Aspekte sind Anonymität, Unverkettbarkeit von Ereignissen, Nichterkennbarkeit, Abstreitbarkeit und Vertraulichkeit.

Der Schutz von Privatsphäre ist meistens in Abhängigkeit von einem hypothetischen Angreifer zu betrachten. Das Ziel des Angreifers ist es, sensible Informationen (wie z.B. dem Aufenthaltsort eines Individuums) in Erfahrung zu bringen. Die Definition des Angreifers erfolgt üblicherweise über dessen Eigenschaften [Dí02]. So kann er anhand verschiedener Dimensionen charakterisiert werden, z.B. intern vs. extern, lokal vs. global, aktiv vs. passiv, statisch vs. adaptiv, oder bzgl. existierendem Vorwissen. Um den Privatsphärenschutz zweier Systeme miteinander vergleichen zu können, muss das zugrunde liegende Angreifermodell identisch sein. Es ist daher unbedingt notwendig, genau zu spezifizieren, unter welchen Rahmenbedingungen welche Art von Privatsphäre und welche Aspekte bewertet wurden.

Der präsentierten Taxonomie folgend beschäftigen sich die Methoden und Evaluierungen in dieser Arbeit hauptsächlich mit der Privatheit des Ortes unter den Aspekten der Anonymität und Unverkettbarkeit, basierend auf den periodisch gesendeten Nachrichten innerhalb eines Ad-Hoc-Fahrzeugnetzes. Als Angreifer wird ein Externer, Passiver, Lokaler angenommen, der szenariospezifisches Wissen hat, d.h. er weiß über die physischen Grenzen der Fahrzeugdynamik Bescheid, ohne jedoch zum Beispiel konkretes Wissen über den Fahrstil einzelner Personen zu verfügen.

Die Notwendigkeit von effektiven Mechanismen zum Privatsphärenschutz in Ad-Hoc-Fahrzeugnetzen wurde früh erkannt, jedoch sind nur wenige dieser Aspekte tatsächlich in die Standards der ETSI oder IEEE eingeflossen [ES14]. Das europäische ETSI ITS-G5 und das amerikanische IEEE WAVE System weisen sehr viele Ähnlichkeiten auf: In beiden Systemen sollen Fahrzeuge, basierend auf dem WLAN-Standard IEEE 802.11p, periodisch mit bis zu 10 Hertz unverschlüsselte Statusnachrichten versenden. Diese Nachrichten können ohne größeren Aufwand von jedem, der sich in Reichweite befindet, abgehört und benutzt werden, um Fahrzeuge virtuell zu verfolgen. Um diesen Missbrauch zu verhindern, sehen beide Standards den Aufbau einer sogenannten Public-Key-Infrastruktur in Verbindung mit Pseudonymen vor.

Dieses System basiert auf asymmetrischer Kryptographie und der Nutzung von Zertifikaten. Alle Zertifikate beinhalten den öffentlichen Schlüssel, eine Gültigkeitsdauer und eine Signatur, zusammen mit der Identität des Signierers. Jedes Fahrzeug ist mit einem Basiszertifikat, den dazugehörigen öffentlichen und privaten Schlüsseln sowie mit dem Zertifikat der Zertifizierungsstelle ausgestattet. Das Basiszertifikat ist von der Zertifizierungsstelle unterschrieben und erlaubt es dem Fahrzeug pseudonyme Zertifikate, oder kurz, Pseudonyme, anzufordern. Für Car-2-X-Kommunikation werden ausschließlich Pseudonyme benutzt und niemals die Basisidentität selbst. Das Pseudonym ist somit die Absenderadresse des Fahrzeuges. Wenn ein Fahrzeug eine unverschlüsselte Nachricht sendet, so werden das aktuell gültige Pseudonymzertifikat und eine Signatur dieser Nachricht, welche mit dem privaten Schlüssel dieses Pseudonyms erstellt ist, angehängt. Das empfangende Fahrzeug prüft dann die Signatur im Pseudonymzertifikat sowie die Signatur der

Nachricht. Durch diese Mechanismen können Integrität und Authentizität der Nachricht sichergestellt werden.

Sollte ein Fahrzeug den Eigentümer wechseln, das Car-2-X-System im Fahrzeug kompromittiert worden sein oder unabsichtlich fehlerhafte Nachrichten gesendet werden, so ist es notwendig alle noch gültigen Pseudonyme des Fahrzeuges zu widerrufen, um einen negativen Einfluss auf andere Fahrzeuge zu verhindern [EDS13]. Der Prozess des Zertifikatswiderrufes stellt selbst eine Herausforderung an den Privatsphärenschutz dar, wie später im Artikel gezeigt wird.

Die bloße Verwendung einer PKI gewährt noch keinen Schutz der Privatsphäre, da z.B. eine zu geringe Wechselfrequenz des Pseudonymes einem Angreifer die Möglichkeit verschafft, ein Fahrzeug über eine gesamte Fahrt hinweg wiederzuerkennen. Es ist daher entscheidend, welche Pseudonymwechselstrategie angewendet wird. Es existieren eine Reihe an Vorschlägen [Pe15], vom Austausch von Pseudonymen zwischen Fahrzeugen, über zeitlich oder örtlich gebundene Pseudonyme, bis hin zu dem Konzept, nach einem Pseudonymwechsel eine kurze Zeit nicht zu senden, um mithörende Angreifer zu verwirren.

Viele dieser Methoden vernachlässigen jedoch, dass Mechanismen zum Privatsphärenschutz keinen negativen Einfluss auf die Verkehrssicherheit haben dürfen und selbst auch keine neuen möglichen Angriffsvektoren mit sich bringen sollten [ES16]. Ein Ziel dieser Arbeit ist es herauszufinden, wie dieser Privacy-Safety-Tradeoff gelöst werden kann, da es scheint, dass bis zum jetzigen Zeitpunkt viele Schutzmechanismen das falsche Ziel verfolgen: Das Verwirren eines mithörenden Angreifers. Dies steht im direkten Widerspruch zum eigentlichen Ziel von Fahrzeugnetzen, nämlich Fahrzeugen in der Nähe zu erlauben eine virtuelle Umgebung aufzubauen, um Unfälle zu vermeiden.

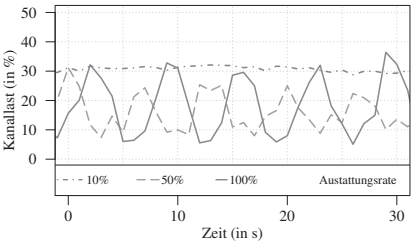
3 Bewertung von Privatsphäre mittels Simulation

Der Einsatz von Simulationswerkzeugen zur Leistungsbewertung von Applikationen und Protokollen im Kontext der Fahrzeugkommunikation ist weit verbreitet. Üblicherweise werden diskrete, mikroskopische, agenten-basierte Simulationsumgebungen eingesetzt, d.h. das Verhalten jedes Fahrzeuges (= Agent) wird autonom bestimmt, woraus sich Effekte auf das Gesamtsystem ergeben. Mikroskopisch bestimmt in diesem Kontext den Abstraktionsgrad. Fahrzeuge bestimmen autonom zu jedem diskreten Zeitschritt ihr Verhalten, wie z.B. Spurwechsel oder Beschleunigung.

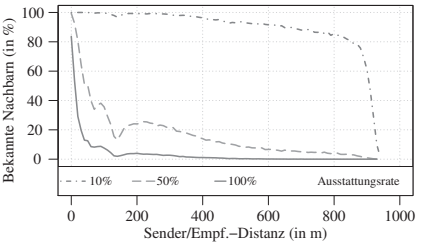
Die Mobilität der Fahrzeuge hat einen entscheidenden Einfluss auf die Netzwerktopologie, und Informationen die von Fahrzeugen empfangen werden, können wiederum Einfluss auf die Mobilität haben. Aus diesem Grund werden Netzwerksimulatoren und Verkehrssimulatoren bidirektional gekoppelt. Im Falle dieser Arbeit sind dies der Netzwerksimulator OMNeT++ und der Verkehrssimulator SUMO.

Eine wichtige Erkenntnis im Rahmen dieser Arbeit ist, dass die eingesetzten Modelle der zugrundeliegenden Funktechnologie einen entscheidenden Einfluss auf die Netztopologie haben können [ESD12], und somit auch direkt auf Mechanismen zum Privatsphärenschutz.

So berücksichtigen diverse Wechselstrategien auch Fahrzeuge in der direkten Umgebung, um zu entscheiden, ob das Pseudonym gewechselt werden soll [Ec11]. Aus diesem Grund wurden für beide Kommunikationsstandards, IEEE WAVE und ETSI ITS-G5, detaillierte Modelle der Medienzugriffsschicht entwickelt [ESG13] und der physische Kanal so gut wie möglich approximiert [So13].



(a) Problem der Kanallastoszillation unter ETSI ITS-G5 bei hoher Ausstattungsrate



(b) Paketkollisionen durch Synchronisierung bei IEEE WAVE führen zu nicht erkannten Nachbarn

Abbildung 1: Exemplarische Ergebnisse der Medienzugriffsmodellierung mit entdeckten Schwachstellen des europäischen und amerikanischen Systems

Zwei weitere wichtige Ergebnisse finden sich in Abbildung 1. Die detailgetreue Modellierung der unteren Schichten ermöglichte die Aufdeckung von Schwachstellen in den Protokollen. Es konnte gezeigt werden, dass die Kanalüberlastkontrolle bei ETSI ITS-G5 zu synchronisierten, starken Oszillationen gesamter Fahrzeugverbünde führen kann (Abbildung 1a), was wiederum zur Folge hat, dass die Kanalkapazität nicht effizient genutzt wird [ESG13]. Dies hat direkten Einfluss auf mögliche Sicherheitsanwendungen. Ähnliche Problematiken treten bei IEEE WAVE auf, jedoch werden diese hier durch den im Standard vorgesehenen periodischen Kanalwechsel hervorgerufen, durch den Fahrzeuge direkt nach dem Kanalwechsel mit einer größeren Wahrscheinlichkeit auf den Kanal zugreifen [ESD12]. In Abbildung 1b erkennt man, dass die daraus resultierenden hohen Paketverluste direkten Einfluss darauf haben, wie viele Fahrzeuge in naher Umgebung erkannt werden. (Beide Erkenntnisse wurden auf sichtbaren Konferenzen präsentiert und auch direkt mit Partnern in den jeweiligen Gremien besprochen, was dazu beitrug, dass Vorschläge zur Behebung dieser Probleme in den Standard einfließen werden.)

Um zu verstehen, welchen Grad an Privatsphärenschutz verschiedene Pseudonymwechselstrategien erreichen, wurde ein modernes Multi-Target-Tracking System entwickelt. Die Idee hierbei ist es, sich in die Rolle des Angreifers zu versetzen und zu versuchen mit den zugrunde liegenden Informationen, sprich den empfangenen Paketen, Fahrzeuge durch das Netzwerk zu verfolgen. Der Angreifer ist so modelliert, dass er verschiedene Empfängerantennen platziert und die unverschlüsselten Übertragungen der Fahrzeuge abhorcht.

Die Problematik und das Prinzip sind in Abbildung 2 dargestellt: Angenommen zwischen Zeitpunkt $t = 2$ und $t = 3$ wechseln Fahrzeuge ihre Pseudonyme, so ist es das Ziel des Angreifers anhand der nun scheinbar anonymen Beobachtungen $o1, o2, o3$ die bereits existierenden Tracks fortzuführen. Ist er in der Lage dies mit hoher Wahrscheinlichkeit zu erreichen, so war dieser Pseudonymwechsel hinsichtlich dieses Angreifers wirkungslos.

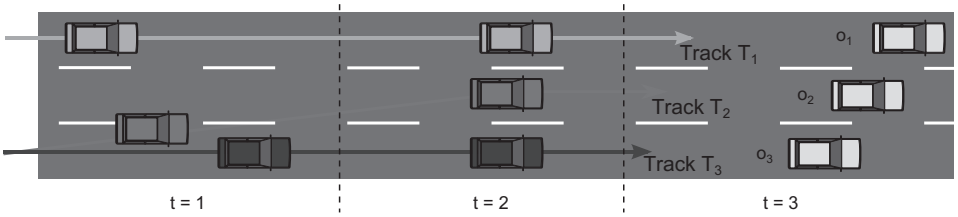
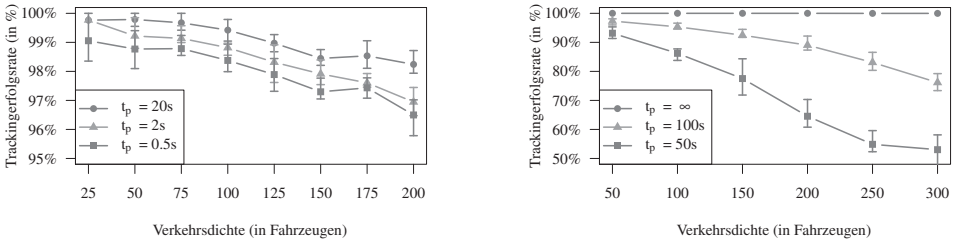


Abbildung 2: Tracking kann verstanden werden als das Problem der Zuordnung von neuen Beobachtungen o_i zu existierenden Tracks T_j.



(a) Vollüberwachtes Kreuzungsszenario

(b) Teilüberwachtes Autobahnszenario

Abbildung 3: Trackingerfolgsrate eines Angreifers bei verschiedenen Pseudonymgültigkeitsdauern t_p. Fehlerbalken zeigen die 25%- und 75%-Quantile über alle Simulationsläufe.

Das entwickelte Trackingsystem wurde mit verschiedenen Pseudonymwechselstrategien aus der Literatur evaluiert. Das entscheidende Ergebnis hierbei ist, dass es selbst auf einer sehr geschäftigen Kreuzung mit hunderten Fahrzeugen nicht möglich ist, einen mithörenden Angreifer zu verwirren, ohne dabei die Verkehrssicherheitsmechanismen des Systems negativ zu beeinflussen. Abbildung 3a zeigt die Ergebnisse für eine vollständig abgedeckte Kreuzung. Ein Fahrzeug gilt als getrackt, wenn der Angreifer es von der Einfahrt in den Kreuzungsbereich bis zum Verlassen virtuell verfolgen kann, sich also nicht von Pseudonymwechseln verwirren lässt. Es ist zu beobachten, dass es selbst unter für die Privatsphäre scheinbar optimalen Bedingungen bei Pseudonymgültigkeitsdauern von $t_p = 0.5s$ und einer Sendefrequenz von 1Hz fast unmöglich ist, einen Angreifer zu verwirren (Tracking-Erfolgsrate von über 95%).

In einem zweiten Szenario wurde der Effekt von Pseudonymwechseln bei Fahrzeugen untersucht, die sich zum Zeitpunkt des Wechsels nicht in Reichweite eines Angreifers befanden. Zu diesem Zweck wurde ein Autobahnabschnitt untersucht, in dem ein Angreifer am Anfang und am Ende eine Empfängerantenne platziert hat. In der Mitte entstand dadurch ein ca. 800 Meter breiter Bereich, in dem der Angreifer keine Pakete empfangen konnte. Fahrzeuge gelten in diesem Szenario als getrackt, wenn der Angreifer in der Lage war Fahrzeuge von Anfang bis zum Ende des Abschnittes zu verfolgen, sie also beim Passieren der zweiten Empfangsantenne wiederzuerkennen. Die Ergebnisse in Abbildung 3b zeigen, dass bei Pseudonymgültigkeitsdauern von 50s (ca. 90% Chance, dass ein Fahrzeug sein Pseudonym im nicht überwachten Bereich wechselt) nur noch 50% aller Fahrzeuge verfolgt werden konnten.

Die bisherige Herangehensweise muss also grundlegend geändert werden. Weg von dem Ziel mithörende Angreifer zu verwirren, hin zu einem Privatsphärenschutz, der effektiv ausnutzt, wenn ein Angreifer nicht mithört. Zusätzlich sollte dieser Schutz niemals die Verkehrssicherheit negativ beeinflussen und außerdem ressourcenschonend bzgl. Speicherplatz im Fahrzeug und Kommunikationsoverhead sein. Im Rahmen dieser Arbeit wurde eine solche Lösung entwickelt, die im nächsten Kapitel vorgestellt wird.

4 Effizienter und praktikabler Privatsphärenschutz

Die Basis des vorgeschlagenen Ansatzes bildet ein Pseudonympool, der aus für alle Fahrzeuge synchronen, nicht überlappenden Zeitschlitzen besteht [Ec11]. Jedes Fahrzeug verwaltet einen solchen Pool und wechselt sein Pseudonym, sobald der nächste Zeitschlitz aktiv wird. An den Zeitschlitzgrenzen ändert folglich jedes Fahrzeug im gesamten Netzwerk sein Pseudonym. Die Konfiguration dieser Pools basiert daher nur auf zwei Parametern: der Größe des Pools sowie der Länge eines Zeitschlitzes.

Nimmt man an, dass alle Fahrzeuge synchrone Uhren haben (z.B. durch GPS), dann ist der Pseudonymwechsel nahezu exakt synchron. Damit diktiert die Zeitschlitzlänge automatisch die Pseudonymwechselstrategie. Dies impliziert des Weiteren, dass alle Fahrzeuge, die zu diesem Zeitpunkt nicht von einem Angreifer überwacht werden können, ein neues, dem Angreifer unbekanntes Pseudonym verwenden. Das erschwert das Tracking, wenn diese Fahrzeuge wieder in einen vom Angreifer überwachten Bereich einfahren und ist eine wichtige Eigenschaft des Systems. Die Verwirrung des Angreifers kann auf diese Weise maximiert werden, was wiederum mit einer Maximierung der Privatsphäre der betroffenen Fahrzeuge gleichzusetzen ist [ES16]. Je kleiner die Zeitschlitzlänge gewählt ist, desto größer ist die Wahrscheinlichkeit, dass ein Fahrzeug sein Pseudonym wechselt, während es sich außerhalb der Reichweite eines Angreifers befindet. Dies ist damit der entscheidende Parameter für die Privatsphäre des Systems.

Ein weiterer Vorteil von nicht überlappenden Zeitschlitzen ist, dass sogenannte Sybil-Angriffe, also Angriffe, bei denen ein Fahrzeug mehrere Fahrzeuge imitiert, nicht mehr möglich sind, weil zu jedem beliebigen Zeitpunkt nur ein valides Pseudonym pro Fahrzeug verfügbar ist. Weiterhin erlaubt das Zeitschlitzverfahren effiziente Pseudonymwiderrufsverfahren, wie anschließend gezeigt wird.

Die Problematik, dass Mechanismen zum Privatsphärenschutz einen negativen Einfluss auf die Verkehrssicherheitsfunktionen der Car-2-X-Systeme haben können, stellt eine große Hürde beim Design dieser Mechanismen dar. Der Ansatz der synchronen Zeitschlitze nimmt den Fahrzeugen die autonome Entscheidung, wann das Pseudonym gewechselt werden soll. Das heißt, alle Fahrzeuge auf einer geschäftigen Kreuzung werden gleichzeitig ihr Pseudonym wechseln, was potentiell (wenn auch mit kleiner Wahrscheinlichkeit) negative Effekte auf die Sicherheit haben kann. Aber selbst wenn diese Wahrscheinlichkeit nur ein Zehn-tausendstel beträgt, so führt die schiere Menge an Fahrzeugen auf der Straße irgendwann zu einem Unfall, der ohne den Schutzmechanismus verhindert werden hätte können.

Die Simulationsstudie in Abschnitt 3 hat gezeigt, dass es fast unmöglich ist, lokale Angreifer zu verwirren. Neuere Studien, die auf Daten aus echten Feldtests basierend, bestätigen diese Ergebnisse [ES16]. Nur wenn die Sendefrequenz auf für Verkehrssicherheit unzureichende Werte gesetzt wird, kann ein mithörender Angreifer verwirrt werden. Jedoch können selbst in diesen Fällen sogenannte Fingerprinting-Angriffe eingesetzt werden, um Fahrzeuge zu verfolgen [Bl15]. Die logische Konsequenz aus diesen Erkenntnissen ist demnach ein System, in dem Pseudonymwechsel lokal bekannt gegeben werden. Das heißt, dass nach jedem Pseudonymwechsel das alte Pseudonym kurz mitgeführt werden muss.

Mit diesem Ansatz wird jeglicher theoretischer Einfluss des Schutzmechanismusses auf die Verkehrssicherheit vermieden. Des Weiteren hat dieser Ansatz nur einen geringen Overhead, da lediglich eine zusätzliche Signaturverifikation pro Fahrzeug in der Umgebung benötigt wird. Sobald ein Fahrzeug kryptographisch beweisen konnte, dass es die privaten Schlüssel für das alte und das neue Pseudonym besitzt, müssen empfangene Fahrzeuge nur noch eine Signatur prüfen. Um ein Fahrzeug anhand dieser Ankündigungen verfolgen zu können, benötigt ein Angreifer entweder globales Wissen über alle gesendeten Nachrichten oder er muss das Fahrzeug physisch verfolgen. Das ist jedoch kein Nachteil des Systems, da ein Hinterherfahren unabhängig von Car-2-X-Kommunikation möglich ist.

Der Einsatz von zeitschlitz-basierten Pseudonympools erlaubt die Einführung von effizienten Mechanismen zum Widerruf von Pseudonymzertifikaten [EDS13]. Anstatt eine Liste mit allen widerrufenden Pseudonymen zu veröffentlichen wird die Berechnung der gesperrten Pseudonyme auf die Fahrzeuge verschoben. Um dies zu erreichen, wird jedem Pseudonym ein sogenannter Verknüpfungswert C_v^i angehängt, wobei i die Zertifikatsnummer und v das Fahrzeug ist.

Diese Verknüpfungswerte sind durch eine kryptographische Hashfunktion $h(\cdot)$ und ein fahrzeugspezifisches Passwort κ_v miteinander verbunden. Der Wert C_v^i kann dann mit Hilfe des Schlüssels κ_v^i und einer bekannten, symmetrischen Verschlüsselungsfunktion $e(\cdot)$ berechnet werden. (Die hier dargestellte Version des Ansatzes beruht auf der Vereinfachung des Systems durch [Wh13], siehe Abbildung 4)

$$\begin{array}{ccccccc} \kappa_v & \xrightarrow{h(\kappa_v)} & \kappa_v^2 & \xrightarrow{h(\kappa_v^2)} & \kappa_v^3 & \xrightarrow{h(\kappa_v^3)} & \cdots \\ \downarrow e(\kappa_v) & & \downarrow e(\kappa_v^2) & & \downarrow e(\kappa_v^3) & & \\ C_v^1 & & C_v^2 & & C_v^3 & & \cdots \end{array}$$

Abbildung 4: Graphische Repräsentation des Zertifikatwiderrufs basierend auf Verknüpfungswerten

Hat ein Fahrzeug v also n Pseudonyme, und die Zertifizierungsstelle CA möchte nur die zukünftigen Pseudonyme $\geq j$ widerrufen, dann wird die Hashfunktion $h(\cdot)$ genau $j-1$ mal auf Fahrzeugpasswort κ_v angewendet. Der resultierende Schlüssel κ_v^j wird anschließend zusammen mit der Anzahl der zu widerrufenden Pseudonyme $n-j$ veröffentlicht.

Somit kann jedes Fahrzeug alle nun widerrufenen Pseudonyme selbst berechnen. Durch die Nichtumkehrbarkeit der kryptographischen Hashfunktion ist es nicht möglich die Verknüpfungswerte für Zertifikate $< j$ zu berechnen. Dies schützt die Privatsphäre der betroffenen Fahrzeuge, da selbst wenn ein Angreifer in der Vergangenheit mitgehörte Pseudonyme gespeichert hat, eine Zuweisung der Pseudonyme zu Fahrzeugen nicht möglich ist.

5 Schlussfolgerung

Die in der zugrunde liegenden Dissertation vorgestellten Methoden und Taxonomien erlaubten es, das Privatsphärenproblem in Fahrzeug-Ad-hoc-Netzen detailliert zu erfassen. Dabei fiel auf, dass viele Lösungsansätze aus der Literatur inkompatibel mit den Rahmenbedingungen von Fahrzeugnetzen sind und es unpraktikabel ist, mithörende Angreifer durch Pseudonymwechsel zu verwirren. Durch die Nutzung von synchronen, nicht überlappenden, zeitschlitz-basierten Pseudonympools und der lokalen Ankündigung von Pseudonymwechseln, kann ein Schutzmechanismus installiert werden, der wenig Overhead aufweist, keinen negativen Einfluss auf Sicherheitsfunktionen mit sich bringt, aber gleichzeitig die Privatsphäre aller Fahrzeuge effektiv schützt. Zusätzlich verhindert dieser Ansatz im Gegensatz zu anderen Vorschlägen aus der Literatur sogenannte Sybilangriffe und erlaubt des Weiteren die Nutzung von effizienten Widerrufsmechanismen.

Literaturverzeichnis

[Bl15] Bloessl, Bastian; Sommer, Christoph; Dressler, Falko; Eckhoff, David: The Scrambler Attack: A Robust Physical Layer Attack on Location Privacy in Vehicular Networks. In: 4th IEEE International Conference on Computing, Networking and Communications (ICNC 2015), CNC Workshop. IEEE, Anaheim, CA, S. 395–400, February 2015.

[Dí02] Díaz, Claudia; Seys, Stefaan; Claessens, Joris; Preneel, Bart: Towards Measuring Anonymity. In: Second International Workshop on Privacy Enhancing Technologies (PET 2002). Jgg. LNCS 2482. Springer, S. 54–68, April 2002.

[Ec11] Eckhoff, David; Sommer, Christoph; Gansen, Tobias; German, Reinhard; Dressler, Falko: SlotSwap: Strong and Affordable Location Privacy in Intelligent Transportation Systems. IEEE Communications Magazine, 49(11):126–133, November 2011.

[EDS13] Eckhoff, David; Dressler, Falko; Sommer, Christoph: SmartRevoc: An Efficient and Privacy Preserving Revocation System Using Parked Vehicles. In: 38th IEEE Conference on Local Computer Networks (LCN 2013). IEEE, Sydney, Australia, S. 855–862, October 2013.

[ES14] Eckhoff, David; Sommer, Christoph: Driving for Big Data? Privacy Concerns in Vehicular Networking. IEEE Security and Privacy, 12(1):77–79, February 2014.

[ES16] Eckhoff, David; Sommer, Christoph: Marrying Safety with Privacy: A Holistic Solution for Location Privacy in VANETs. In: 8th IEEE Vehicular Networking Conference (VNC 2016). Columbus, OH, USA, December 2016.

[ESD12] Eckhoff, David; Sommer, Christoph; Dressler, Falko: On the Necessity of Accurate IEEE 802.11p Models for IVC Protocol Simulation. In: 75th IEEE Vehicular Technology Conference (VTC2012-Spring). IEEE, Yokohama, Japan, S. 1–5, May 2012.

[ESG13] Eckhoff, David; Sofra, Nikoletta; German, Reinhard: A Performance Study of Cooperative Awareness in ETSI ITS G5 and IEEE WAVE. In: 10th IEEE/IFIP Conference on Wireless On demand Network Systems and Services (WONS 2013). IEEE, Banff, Canada, S. 196–200, March 2013.

[Eu95] European Parliament: Directive 95/46/EC. Official Journal, L 281:0031–0050, November 1995.

[FWF13] Finn, Rachel L; Wright, David; Friedewald, Michael: Seven Types of Privacy. In (Gutwirth, Serge; Leenes, Ronald; de Hert, Paul; Poullet, Yves, Hrsg.): European Data Protection: Coming of Age. Springer, S. 3–32, 2013.

[Ni04] Nissenbaum, Helen: Privacy as Contextual Integrity. Washington Law Review, 79(1):119–158, June 2004.

[Pe15] Petit, Jonathan; Schaub, Florian; Feiri, Michael; Kargl, Frank: Pseudonym Schemes in Vehicular Networks: A Survey. IEEE Communications Surveys & Tutorials, 17(1):228–255, March 2015.

[PH10] Pfitzmann, Andreas; Hansen, Marit: , A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, August 2010. v0.34.

[SHG03] Schilit, B.; Hong, J.; Gruteser, M.: Wireless Location Privacy Protection. Computer, 36(12):135–137, December 2003.

[So13] Sommer, Christoph; Joerer, Stefan; Segata, Michele; Tonguz, Ozan K.; Lo Cigno, Renato; Dressler, Falko: How Shadowing Hurts Vehicular Communications and How Dynamic Beaconing Can Help. In: 32nd IEEE Conference on Computer Communications (INFOCOM 2013), Mini-Conference. IEEE, Turin, Italy, S. 110–114, April 2013.

[We67] Westin, Alan: Privacy and Freedom. Atheneum, 1967.

[Wh13] Whyte, William; Weimerskirch, Andre; Kumar, Virendra; Hehn, Thorsten: A Security Credential Management System for V2V Communications. In: 5th IEEE Vehicular Networking Conference (VNC 2013). IEEE, Boston, MA, S. 1–8, December 2013.

David Eckhoff arbeitet als Postdoc bei TUMCREATE in Singapur, einem gemeinsamen Forschungsinstitut der TU München und der Nanyang Technological University Singapur. In 2009 schloss er sein Diplom (Dipl.-Inf. Univ.) als bester seines Jahrgangs ab und promovierte anschließend mit Auszeichnung (Dr.-Ing.) im Jahr 2016 bei Prof. Reinhard German an der Universität Erlangen. Im Jahr 2016 arbeitete er als Gastwissenschaftler in der Gruppe von Prof. Lars Kulik an der Universität Melbourne in Australien. Im Oktober 2016 trat er eine Stelle bei TUMCREATE in Singapur in der Gruppe von Prof. Alois Knoll an. Seine Forschungsinteressen beinhalten Datenschutz, Smart Cities, Fahrzeugnetze und intelligente Transportsysteme mit dem Fokus auf Modellierung und Simulation.