Eine Experimentierumgebung zur Studie der physikalischen Schicht einer WLAN-Variante für die Anwendung in Fahrzeugnetzen[1]

Bastian Bloessl[2]

Abstract: Zukünftig werden Automobile mit Kommunikationsmodulen ausgestattet, die einen direkten Datenaustausch zwischen Fahrzeugen ermöglichen. Auf diese Weise können sich Verkehrsteilnehmer koordinieren, um so den Straßenverkehr sicherer, effizienter und komfortabler zu gestalten. Eine der Technologien, die dafür in Betracht gezogen wird, ist IEEE 802.11p, eine an Fahrzeugnetze angepasste Version von Wireless LAN (WLAN). Um die Eignung des Standards in diesem von der normalen WLAN-Nutzung sehr unterschiedlichen Umfeld zu untersuchen, haben wir prototypisch einen Software Defined Radio (SDR)-basierten IEEE 802.11p Transceiver implementiert. SDRs, programmierbare Funksende- und -empfangseinheiten, erlauben vollen Zugriff auf alle Aspekte drahtloser Kommunikation, bis hin zur elektromagnetischen Wellenform, und sind damit prädestiniert, die physikalische Schicht zu untersuchen. Eine Besonderheit unserer Implementierung besteht darin, dass wir durch abbilden des Standards in Software, dieselbe Implementierung für Simulationen und Messungen nutzen können, was eine detaillierte und umfassende Untersuchung erlaubt. Um die Vorteile und den flexiblen Einsatz unseres Transceivers herauszustellen, gehen wir auf zwei Studien ein, die ohne eine SDR-Implementierung nicht möglich gewesen wären. Zum einen untersuchen wir den Einfluss von Interferenz auf IEEE 802.11p und validieren so ein in vielen Studien genutztes Simulationsmodell. Zum anderen stellen wir einen neuen Angriff auf die Privatsphäre in Fahrzeugnetzen vor, der erst durch die Möglichkeit auf alle Daten des Empfangsprozesses zuzugreifen realisiert werden kann.

1 Einführung

Schon heute erleben wir, wie autonome Fahrzeuge dabei sind den Verkehr, und damit große Teile unserer Gesellschaft, zu revolutionieren. Viele der grundlegenden Fragestellungen sind gelöst und die ersten Prototypen fahren auf Deutschlands Straßen. Zukünftig werden wir noch einen Schritt weiter gehen und Fahrzeuge mit Funkmodulen ausstatten, um durch Kommunikation untereinander und optional auch mit fest installierten Infrastrukturknoten ein Fahrzeugnetz aufzubauen. Damit ermöglichen wir die Weiterentwicklung vom autonomen zum kooperativem Fahren. Wenn wir uns ins Gedächtnis rufen wie revolutionär die Möglichkeit der Vernetzung bei Computern, und später dem Smartphone, war, können wir abschätzen, was diese Entwicklung für den Verkehr bedeuten kann. So schaffen Fahrzeugnetze die Grundlage für eine Vielzahl von Anwendungen, die häufig unter Cooperative

[1] Eine Kurzfassung der Dissertation: B. Bloessl: A Physical Layer Experimentation Framework for Automotive WLAN, PhD Thesis (Dissertation), Paderborn, Germany: Department of Computer Science, Juni 2018.

[2] Connect Center, Trinity College Dublin, Ireland, E-Mail: mail@bastibl.net.

Intelligent Transportation Systems (C-ITS) zusammengefasst werden. Heute beschäftigen sich Forscher zum Beispiel mit Systemen zur Warnungen vor Querverkehr, verteilen Verkehrsinformationssystemen und automatisiertem Fahren in geringem Abstand [SD14]. Durch Anwendungen wie diesen werden Fahrzeugnetze den Verkehr in Zukunft sicherer, effizienter und komfortabler gestalten. Allein anhand der Vielfalt der möglichen Applikationen gibt es keine Technologie, die allen Anforderungen gerecht werden kann. Fahrzeugnetze werden deshalb mit großer Wahrscheinlichkeit heterogen aufgebaut sein und einen Mix aus Technologien, wie etwa LTE, WLAN, Millimeter Wave (mmW) und Visible Light Communication (VLC), verwenden.

1.1 Grundlagen

Eine zentrale Rolle könnte dabei IEEE 802.11p spielen. IEEE 802.11p ist eine an die Anforderungen in Fahrzeugnetzen angepasste Version von WLAN, die auf einem dedizierten Frequenzband um 5.9 GHz operiert. Mit diesem Standard können Fahrzeuge auch direkt miteinander kommunizieren und so ein dezentrales Netz, ein Vehicular Ad Hoc Network (VANET), bilden. Der IEEE 802.11p-Standard ist vor Allem relevant, weil er Vorteile bietet, die ihn besonders für Anwendungen aus dem Sicherheits- und Effizienzbereich geeignet erscheinen lassen:

Geringe Kosten: Es nutzt günstige, in großen Mengen produzierte Chips, die auf einem dedizierten, frei zugänglichen Frequenzband operieren.

Niedrige Latenz: Es unterstützt direkte Kommunikation zwischen Fahrzeugen und ist nicht auf eine Basisstation oder einen anderen Netzzugangsknoten angewiesen.

Hohe Reichweite: Es ermöglicht Reichweiten von über 800 m [GAS06] und ist nicht auf eine direkte Sichtverbindung angewiesen oder wird von Regen geblockt.

Keine Direktionalität: Im Gegensatz zu VLC und mmW hat WLAN keine inhärente Direktionalität und ist deswegen gut für broadcast-basierte Kommunikation zu allen Fahrzeugen in der Umgebung geeignet.

Angesichts dieser Eigenschaften und der Tatsache, dass Sicherheits- und Effizienzanwendungen als eine der wichtigsten Argumente für die Einführung von C-ITS angeführt werden, ist es wahrscheinlich, dass die Technologie eine zentrale Rolle in zukünftigen Fahrzeugnetzen spielen wird. Ihr derzeit größter Konkurrent ist Cellular Vehicle-to-Everything (C-V2X), eine im GPP-Umfeld entwickelter Kommunikationsstandard, der in LTE Release 14 aufgenommen wurde [WMG17]. C-V2X bietet ähnliche Vorteile und entwickelt sich rasch weiter, ist aber im Vergleich zu IEEE 802.11p weniger gut erforscht. Welche der beiden Technologien sich durchsetzt wird die Zukunft zeigen.

Im Gegensatz zu C-V2X wurde die physikalische Schicht von IEEE 802.11p initial nicht für die Anwendung in Fahrzeugnetzen konzipiert. Verglichen mit einem IEEE 802.11a/g-Signal wurde lediglich die Bandbreite von 20 MHz auf 10 MHz reduziert. Diese Reduzierung der Bandbreite führt zu einer Dehnung im Zeitbereich, was das Signal robuster in Kanälen mit starker Mehrwegeausbreitung macht. Die Frage, die sich hier anschließt, ist jedoch, ob diese Änderung ausreicht, um zuverlässige Kommunikation in den im Vergleich zu normalem WLAN viel dynamischeren Fahrzeugnetzen zu ermöglichen. In der Literatur wurde das Thema häufig aufgegriffen [AHG07; Fe12; Me11; NBS14]. Und auch heute ist die Eignung der Technologie und die Implementierung von leistungsfähigen Empfängern das Thema vieler Studien.

Ein Problem in diesem Kontext ist die Methodik. Simulationen der physikalischen Schicht basieren beispielsweise häufig auf vielen Annahmen und können deswegen unter Umständen nicht vollkommen überzeugen. Ein Versuch mit echter Hardware hingegen ist aufwendig und unflexibel. Zudem sind die in den Chips verwendeten Algorithmen meist nicht bekannt und können nicht verändert werden. Die Eignung dieser Prototypen als Experimentier- und Forschungsplattform ist deswegen stark eingeschränkt.

1.2 Wissenschaftlicher Beitrag

Um die Nachteile bestehenden Tools zu überwinden, haben wir einen SDR-basierten Prototypen des IEEE 802.11p-Standards implementiert. SDRs sind programmierbare Funksende- und Empfangseinheiten, die beliebige elektromagnetische Wellenformen senden und empfangen können. Sie sind damit das perfekte Werkzeug, um neue Technologien zu entwickeln, prototypisch Umzusetzen und experimentell erproben zu können. Unsere Transceiver nutzt GNU Radio, eine Echtzeit-Signalverarbeitungs-Umgebung die es erlaubt Kommunikationsstandards in Software auf einem normalen PC zu implementieren. So können Kommunikationssyteme schnell und mit relativ wenig Aufwand in Hochsprachen wie C++ und Python programmiert werden [Sk16]. Durch Implementierung des Standards in Software sind wir nicht an eine Hardware oder ein Betriebssystem gebunden. Unser Transceiver funktioniert mit allen SDRs, die von GNU Radio unterstützt werden, und kann zum Beispiel auch auf ARM-Plattformen genutzt werden. Er ist außerdem modular aufgebaut, das heißt Algorithmen können auf einfache Weise ausgetauscht und so verschiedene Empfängerarchitekturen miteinander verglichen werden. Die Implementierung wurde sowohl simulativ als auch mit kommerziellen WLAN-Karten und IEEE 802.11p-Prototypen validiert. Um zu zeigen, dass die Komplexität nicht die Rechenleistung eines PCs übersteigt, haben wir darüber hinaus Tests mit einem voll belegten Kanal durchgeführt. Hier wurde keine Überlast festgestellt.

Der größte Nachteil des Implementierens der physikalische Schicht auf dem PC ist die Latenz. Zum einen müssen die Daten zwischen dem SDR und dem PC übertragen werden, zum anderen werden sie auf einem Betriebssystem verarbeitet, das nicht auf Echtzeitanwendungen optimiert ist. Zeitkritische Funktionen sind deswegen nicht ohne Weiteres umsetzbar. Im

Rahmen der Arbeit haben wir gezeigt, dass durch Auslagern von Funktionalität auf den FPGA des SDR, Kanalzugriff und automatisiertes Anpassen der Empfangsverstärkung realisiert werden können ohne die Vorteile einer PC-Implementierung aufzugeben.

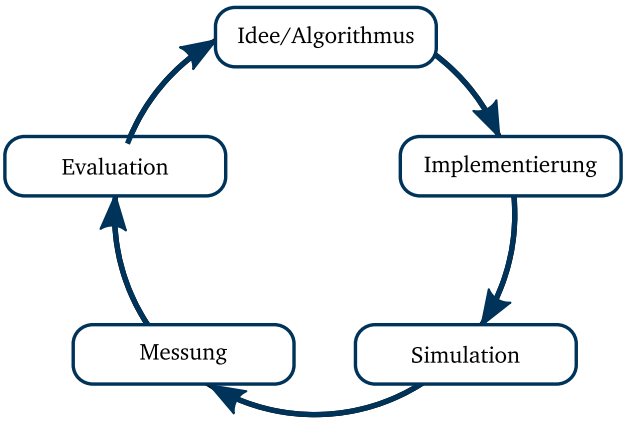

Abb. 1: Unser SDR-basierter Transceiver kann sowohl in Simulationen als auch in Messungen genutzt werden und ermöglicht einen einzigartigen Forschungsprozess, der so mit anderen Werkzeugen nicht möglich ist.

Der größte Vorteil unserer Implementierung ist, dass sie den in Abb. 1 skizzierten Forschungsprozess ermöglicht. Er beginnt mit einer Idee, wie etwa einer Variation des Standards oder eines neuen Signalverarbeitungs-Algorithmus. Diese Idee wird basierend auf unserer Implementierung realisiert und danach zunächst in Simulationen mit verschiedenen Kanalmodellen getestet. Anschließend wird ein und die selbe Implementierung mit SDRs für Messungen im Labor oder in einem Feldtest genutzt. Sollten die Ergebnisse nicht den Erwartungen entsprechen, kann das Design überdacht und die Forschungsfrage iterativ bearbeitet werden. Dieser Prozess ist so mit anderen Werkzeugen nicht möglich. Simulationen sind auf ihre Domäne beschränkt und können nicht für Messungen verwendet werden. Prototypen hingegen sind wenig flexibel und auf Messungen beschränkt. Unsere Implementierung erlaubt einen nahtlosen Übergang zwischen Simulation und Messung, und schafft es so die beiden Domäne zu verbinden. Damit ermöglichen wir ein tiefgreifenderes Verständnis und genauere Leistungsbewertung der WLAN-Technologie in Fahrzeugnetzen.

Insgesamt können die wissenschaftlichen Beiträge der Arbeit wie folgt zusammen gefasst werden:

- Wir entwickeln einen Open-Source SDR-basierten WLAN Transceiver, untersuchen seine Komplexität durch Laufzeittests und validieren ihn in Interoperabilitätstests mit anderen IEEE 802.11p prototypen.
- Wir zeigen, dass es möglich ist, auch zeitkritische Funktionen wie Kanalzugriff oder eine automatische Anpassung der Empfangsverstärkung zu verwirklichen, ohne die Vorteile einer PC-Implementierung aufgeben zu müssen.

Mit Hilfe des Transceivers bearbeiten wir offene Forschungsfragen:

- Wir führen zwei Feldtests durch, in denen wir zum einen die Leistung unserer Implementierung mit anderen Prototypen vergleichen und zum anderen die Tauglichkeit verschiedener Empfangsalgorithmen zu analysieren.
- Wir charakterisieren die Einfluss von Noise und Interferenz auf IEEE 802.11p und validieren so ein häufig verwendetes Simulationsmodell.
- Wir zeigen wie Informationen, die nur mit einer SDR-Implementierung zugänglich sind, genutzt werden können, um ein Bewegungsprofil von Fahrzeugen zu erstellen und quantifizieren die Auswirkungen dieses neuartigen Angriffs auf die Privatsphäre durch Simulationen.

Im Folgenden gehen wir kurz auf zwei Arbeiten ein, die durch diesen SDR-basierten Transceiver ermöglicht wurden.

2 Einfluss von Noise und Interferenz auf IEEE 802.11p

Für makroskopische Studien von Fahrzeugnetzen werden häufig Netzwerksimulatoren eingesetzt. Diese Simulatoren sind gut geeignet, um VANET-Anwendungen zu entwickeln und zu testen, da sie es erlauben auch große Szenarien einfach und reproduzierbar zu betrachten. Wie realistisch und aussagekräftig die Ergebnisse solcher Simulationen sind, hängt maßgeblich von der Qualität der verwendeten Simulationsmodelle ab. Besonders wichtig ist hier das Modell der physikalischen Schicht, das entscheidet, ob eine Übertragung bei gegebenem Signal-, Interferenz- und Noiselevel erfolgreich war. Populäre Simulatoren, wie ns-3 und Veins, nutzen hierfür Fehlerkurven basierend auf dem NIST-Model, das Framelänge, Kodierung und Signal to Interference and Noise Ratio (SINR) auf eine Fehlerwahrscheinlichkeit abbildet. Das Modell ist analytisch abgeleitet und empirisch mit kommerzieller Hardware verifiziert.

Die Krux des Modells ist die Verwendung der SINR. In ihm steckt die implizite Annahme, dass sich Noise und Interferenz in gleicher Weise auf die Fehlerwahrscheinlichkeit auswirken. Im Hinblick darauf, dass das Modell zunächst für das 2.4 GHz-Band mit vielen verschiedenen Interferenzquellen genutzt wurde, mag diese Annahme sinnvoll erscheinen. Da IEEE 802.11p auf einem dedizierten Band arbeitet, treten hier jedoch nur Interferenzen mit anderen IEEE 802.11p-Übertragungen auf. Deswegen und auch aufgrund der Tatsache, dass unabhängige Studien nahelegen, dass sich der Einfluss von Noise und Interferenz unterscheiden [FR15], wollen wir diese Annahme genauer untersuchen.

Mit Hilfe unseres SDR-Transceivers haben wir Simulationen aufgesetzt, in denen ein 546 Byte, QPSK-½-kodierter Frame einmal durch weißes Rauschen und ein anderes mal von einem interferierenden IEEE 802.11p-Frame gestört wurde. Die Störung setzte in

beiden Fällen etwas verzögert ein (nach 122 µs), so bleibt die Synchronisierungssequenz intakt und wir isolieren den Effekt auf die Datensymbole. Um Fehlerkurven zu erzeugen, wurde die relative Energie der beiden Übertragungen variiert und so unterschiedliche SINRs konfiguriert. Zu unserer Überraschung konnten wir zwischen beiden Szenarien keine wesentlichen Unterschiede feststellen. Um dieses Ergebnis zu verifizieren, haben wir dasselbe Szenario zusätzlich mit realer Hardware getestet. Wir senden mit dem SDR das gemixte Signal aus Frame und Noise beziehungsweise Interferenz und nutzen eine kommerzielle WLAN-Karte als Empfänger.

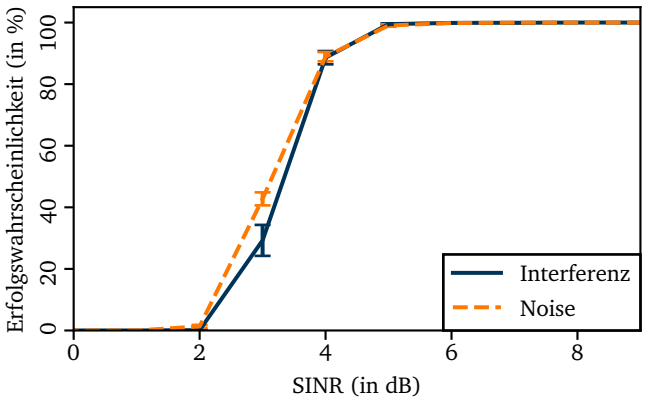

Abb. 2: Erfolgswahrscheinlichkeit für die Übertragung eines Frames, der durch einen anderen Frame, bzw. durch entsprechende Noise, gestört wird. (Reproduziert von [Bl17], © 2017 IEEE.)

Die Ergebnisse dieses Versuchs sind in Abb. 2 zu sehen. Die Fehlerbalken in dieser und der folgenden Abbildung entsprechend Konfidenzintervallen mit einem Signifikanzniveau von 95 %. Auch hier stimmen beide Szenarios sehr gut überein und unterstützen damit die häufig verwendete Annahme, dass Noise und Interferenz einen gleichen, beziehungsweise sehr ähnlichen, Einfluss auf die Leistung der physikalischen Schicht haben. In der Arbeit finden sich weitere Experimente und eine detaillierte Diskussion der Ergebnisse.

Um die Flexibilität unseres SDR-Transceivers zu zeigen, gehen wir im Folgenden über die bloße Leistungsbewertung der physikalischen Schicht hinaus und stellen einen neuartigen Angriff auf die Privatsphäre vor, der durch vollen Zugriff auf den Dekodierprozess ermöglicht wird.

3 Auswirkungen deterministischer Scrambler-Seeds

Bei der Entwicklung von Kommunikationsprotokollen für VANETs, also beispielsweise ETSI ITS-G5 in Europa und IEEE 1609 Wave in den USA, wurde die Privatsphäre von Grund auf mitgedacht. Durch Vermeidung von permanenten Identifikationsmerkmalen wie MAC-Adressen soll verhindert werden, dass auf einfache Weise ein Bewegungprofil von Fahrzeugen erstellt werden kann. Um temporäre Identitäten zu erlauben, werden Pseudonyme

verwendet werden. Diese Pseudonyme sind einmalig und über eine Zertifikatsinfrastruktur zentral verwaltet. Ob dieses Verfahren ausreicht, um die Privatsphäre von Nutzern zu schützen, wird aktuell diskutiert. Unabhängig davon unterstreicht die Debatte aber das Ziel Massenüberwachung zu vermeiden oder zumindest zu erschweren.

Zur Identifikation von Geräten aufgrund spezifischer Charakteristika ihrer Aussendungen gibt es viele Arbeiten. Hier werden jedoch oft kleine Abweichungen der analogen Radiokomponenten genutzt. Verglichen damit ist unser Angriff wesentlicher robuster, da er eine Initialisierungssequenz der physikalischen Schicht nutzt, die von jedem Empfänger am Anfang der Übertragung dekodiert werden muss. Konkret nutzen wir Schwächen der Scrambler-Implementierung. In digitalen Kommunikationssystemen werden die Daten vor der Modulation häufig gescramblt, also mit Hilfe einer pseudo-zufälligen Bitfolge randomisiert. Unabhängig von eventuell vorhandenen Strukturen in den Nutzdaten, also etwa langen Folgen von Nullen oder Einsen, hat die so entstehende gescramblte Bitfolge eine unkorrelierte Gleichverteilung. Diese Randomisierung ist kein Sicherheitsmerkmal, sie wird ausschließlich wegen Vorteilen bei der Signalverarbeitung durchgeführt.

Beim WLAN wird diese Zufallsbitfolge mit einem rückgekoppelten Schieberegister erzeugt, das laut Standard für jeden Frame mit einem pseudozufälligen Seed initialisiert werden soll. Um dem Empfänger das Dekodieren zu ermöglichen, wird der Seed vor den Nutzdaten gesendet. Da der Scrambling-Prozess tief in der physikalischen Schicht verankert ist, kann er mit normalem Netzwerkmonitoring, zum Beispiel mit Wireshark, nicht nachvollzogen werden. Mit unserer SDR-Implementierung ist es hingegen leicht möglich, da der Seed sowieso im Zuge des Dekodier-Prozesses ermittelt werden muss. Um zu sehen wie, die vom Standard geforderte Zufällige Initialisierung Implementiert ist, haben wir mit Hilfe des SDR die Sequenzen für zwei populäre IEEE 802.11p-Prototypen geloggt.

Zum einen untersuchen wir eine, auf einem Atheros AR5413-Chip basierende, Unex DCMA-86P2-Karte, die in vielen Feldtests genutzt wurde. Zum anderen untersuchen wir mit dem Cohda Wireless MK2 einen kommerziellen IEEE 802.11p-Prototypen, der vor allem zum Testen von VANET-Anwendungen weite Verbreitung findet. Bei der Betrachtung der Scrambler-Seeds konnten wir feststellen, dass beide Karten einfache und, was noch schlimmer ist, deterministische Seeds verwenden.

Bei der Atheros-Karte werden die Seeds einfach inkrementiert, es werden also Frames mit Seed 1, 2, 3, ... versendet. Das MK2 hingegen reinitialisert den Scrambler nicht. Auch hier kann ein Angreifer, der einen Frame empfangen hat, den nächsten Seed vorhersagen, da er den Zustand des Schieberegisters kennt. Ist außerdem die Framelänge bekannt, so kann der Angreifer zukünftige Seeds vorhersagen. Bei Atheros-Karten ist das unabhängig von der Framelänge immer möglich. Dieses deterministische Verhalten ist im Hinblick auf die Leistung des Transceivers völlig unkritisch. Mit Blick auf die Privatsphäre ergibt sich jedoch ein anderes Bild, da die Schwächen der Implementierungen eine einfache Zuordnung von Frames zu einem Sender erlauben. Werden etwa Frames mit Scrambler-Seeds von 10, 11, 12, 13, ... empfangen, so ist klar, dass diese mit großer Wahrscheinlichkeit von einem

Fahrzeug mit einer Atheros-Karte stammen. Diese Möglichkeit, Frames unabhängigen von MAC-Adressen oder Pseudonymen einem Empfänger zuzuordnen, hebelt den Schutz der Privatsphäre zum großen Teil aus.

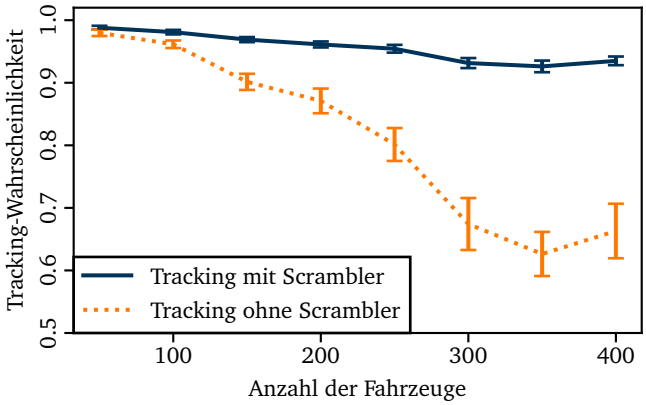

Abb. 3: Einfluss determinstischer Scrambler-Seeds auf die Tracking-Wahrscheinlichkeit. (Reproduziert von [Bl15], © 2015 IEEE.)

Um die Auswirkungen dieser Schwächen zu quantifizieren, haben wir verschiedene Szenarien mit Veins, einem Netzwerksimulator für Fahzeugnetze untersucht. In Abb. 3 werden exemplarisch die Ergebnisse für ein Autobahnszenario gezeigt. Hier werden an einer dreispurigen Autobahn statische Knoten platziert, zwischen denen ein 800 m langer blinder Fleck ist, an dem keiner der Knoten Daten empfangen kann. Die Fragestellung ist hier, ob die Knoten Fahrzeuge zuordnen und damit tracken können. Wir nehmen an, die Fahrzeuge nutzen jeweils zu ⅓, wirklich zufällige, inkrementelle und uninitialisierte Scrambler-Seeds. Die Abbildung vergleicht die Erfolgswahrscheinlichkeit abhängig vom Verkehrsaufkommen. Für die Zuordnung von Fahrzeugen nutzen wir einen dem aktuellen Stand der Forschung entsprechenden Tracking-Algorithmus und vergleichen die Standardversion (orange) mit einer erweiterten Version, die zusätzlich deterministische Seeds ausnutzt (blau). (Weitere Details zum Simulationssetup und finden sich in der Arbeit.) Wie die Abbildung zeigt, können vor allem bei höheren Verkehrsaufkommen die Schwächen in der Scrambler-Implementierung die Tracking-Wahrscheinlichkeit signifikanten erhöhen. Wenn sich durchschnittlich 350 Fahrzeuge auf dem simulierten Autobahnabschnitt befinden, steigt die Tracking-Wahrscheinlichkeit beispielsweise von ca. 63 % auf ca. 95 %.

Inzwischen wurden unsere Untersuchungen von einer unabhängigen Gruppe auch auf andere kommerzielle WLAN-Karten ausgeweitet [Va16]. Auch bei diesen Karten wurden ähnliche Schwachstellen gefunden. Unserer Meinung nach ist es wichtig möglichst frühzeitig auf diese Problematik hinzuweisen, da die physikalische Schicht oft auf dem Chip implementiert ist und die Schwächen unter Umständen nicht durch spätere Firmware-Updates behoben werden können.

4 Schlussfolgerung

Schon in naher Zukunft werden Autos mit Funkmodulen ausgestattet, die eine direkte Kommunikation untereinander ermöglichen und damit die Grundvorraussetzung zum kooperativen Fahren schaffen. Um die Leistungsfähigkeit dieser Technologie besser zu verstehen und ihre Einsatzfähigkeit zu untersuchen, sind Experimente mit Prototypen von entscheidender Bedeutung. In dieser Arbeit haben wir einen SDR-basierten Transceiver entwickelt, der sowohl simulative als auch experimentelle Leistungsbewertung erlaubt und so einen einzigartigen Forschungsprozess ermöglicht. Wir denken, dass diese Implementierung einen wichtigen Beitrag leistet um die Eignung von WLAN-Technologie für Fahrzeugnetze zu evaluieren. Unsere Implementierung wurde mit Hilfe von Simulationsmodellen und Interoperabilitätstests mit IEEE 802.11p-Prototypen validiert. Darüber hinaus wurde gezeigt, dass zeitkritische Funktionen auf den FGPA des SDR ausgelagert werden können, ohne die Vorteile einer PC-Implementierung aufzugeben. Die Flexibilität des Transceivers wurde in Feldtests und zwei weiterführenden Studien gezeigt: Einerseits haben wir den Einfluss von Noise und Interferenz auf IEEE 802.11p untersucht und so ein häufig verwendetes Simulationsmodell validiert. Andererseits haben wir einen neuen Angriff auf die Privatsphäre vorgestellt, der erst durch unsere SDR-Implementierung ermöglicht wurde.

Um unser Arbeit der wissenschaftlichen Gemeinde zur Verfügung zu stellen, wurde der Transceiver unter einer Open-Source-Lizenz veröffentlicht.[3] Inzwischen basieren 72 Veröffentlichungen auf dieser Arbeit. 48 davon wurden von unabhängigen Gruppen publiziert.

Literaturverzeichnis

[AHG07] Alexander, P.; Haley, D.; Grant, A.: Outdoor Mobile Broadband Access with 802.11. IEEE Communications Magazine 45/11, Nov. 2007.

[Bl15] Bloessl, B.; Sommer, C.; Dressler, F.; Eckhoff, D.: 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, Feb. 2015.

[Bl17] Bloessl, B.; Klingler, F.; Missbrenner, F.; Sommer, C.: A Systematic Study on the Impact of Noise and OFDM Interference on IEEE 802.11p. In: 9th IEEE Vehicular Networking Conference (VNC 2017). IEEE, Torino, Italy, Nov. 2017.

[Bl18] Bloessl, B.: A Physical Layer Experimentation Framework for Automotive WLAN, PhD Thesis (Dissertation), Paderborn, Germany: Department of Computer Science, Juni 2018.

[3] `https://www.wime-project.net`

[Fe12] Fernandez, J. A.; Borries, K.; Cheng, L.; Vijaya Kumar, B. V. K.; Stancil, D. D.; Bai, F.: Performance of the 802.11p Physical Layer in Vehicle-to-Vehicle Environments. IEEE Transactions on Vehicular Technology 61/1, Jan. 2012.

[FR15] Fuxjaeger, P.; Ruehrup, S.: Validation of the NS-3 Interference Model for IEEE802.11 Networks. In: 8th IFIP Wireless and Mobile Networking Conference (WMNC 2015). IEEE, Munich, Germany, Okt. 2015.

[GAS06] Gallagher, B.; Akatsuka, H.; Suzuki, H.: Wireless Communications for Vehicle Safety: Radio Link Performance and Wireless Connectivity Methods. IEEE Vehicular Technology Magazine 1/4, Dez. 2006.

[Me11] Mecklenbräuker, C. F.; Molisch, A. F.; Karedal, J.; Tufvesson, F.; Paier, A.; Bernadó, L.; Zemen, T.; Klemp, O.; Czink, N.: Vehicular Channel Characterization and its Implications for Wireless System Design and Performance. Proceedings of the IEEE 99/7, Juli 2011.

[NBS14] Nagalapur, K. K.; Brännström, F.; Ström, E. G.: On Channel Estimation for 802.11p in Highly Time-Varying Vehicular Channels. In: IEEE International Conference on Communications (ICC 2014). IEEE, Sydney, Australia, Juni 2014.

[SD14] Sommer, C.; Dressler, F.: Vehicular Networking. Cambridge University Press, 2014.

[Sk16] Sklivanitis, G.; Gannon, A.; Batalama, S. N.; Pados, D. A.: Addressing Next-Generation Wireless Challenges with Commercial Software-Defined Radio Platforms. IEEE Communications Magazine 54/1, Jan. 2016.

[Va16] Vanhoef, M.; Matte, C.; Cunche, M.; Cardoso, L. S.; Piessens, F.: Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms. In: 11th ACM Asia Conference on Computer and Communications Security (ASIACCS 2016). ACM, Xi'an, China, Mai 2016.

[WMG17] Wang, X.; Mao, S.; Gong, M. X.: An Overview of 3GPP Cellular Vehicle-to-Everything Standards. GetMobile: Mobile Computing and Communications 21/3, Sep. 2017.

Bastian Bloessl ist PostDoc am Trinity College Dublin in Irland, wo er durch ein Marie Skłodowska-Curie-Stipendium finanziert ist. Bastian hat den Diplomstudiengang Informatik an der Universität Würzburg 2011 abgeschlossen. Im selben Jahr begann er seine Promotion in der Gruppe von Prof. Falko Dressler an der Universität Innsbruck, die er ab 2014 in an der Universität Paderborn weiterführte. 2015 erhielt Bastian ein FitWeltweit-Stipendium des DAAD, das es ihm ermöglichte, sechs Monate als Gastwissenschaftler an der University of California, Los Angeles (UCLA) in der Gruppe von Prof. Mario Gerla zu arbeiten. Seit 2017 ist Bastian außerdem einer der Leiter des GNU Radio Projekts, einem Open-Source-Softwareprojekt zur Echtzeitsignalverarbeitung.