# Secure Communication in Inter-Vehicle Networks

Elmar Schoch

Institut für Medieninformatik
Universität Ulm
elmar.schoch@uni-ulm.de

**Abstract:** Fahrzeug-Fahrzeug-Kommunikation gilt als vielversprechende Technologie zur Umsetzung zukünftiger, innovativer Fahrzeugfunktionen. Durch die Einführung der drahtlosen Schnittstelle und neuer Kommunikationsprotokolle zur Unterstützung der Anwendungen entsteht jedoch auch ein nicht vernachlässigbares Missbrauchspotential. Sicherheit und Datenschutz müssen bei der Entwicklung der Technologie von vornherein berücksichtigt werden. Diese Arbeit befasst sich mit der Thematik der Sicherheit gegenüber manipulativen Angriffen auf die Kommunikation. Dazu werden Kommunikationsverfahren auf ihre Schwachstellen hin untersucht und geeignete Sicherheitsmechanismen vorgeschlagen. Dem automobilen Anwendungsbereich Rechnung tragend liegt der Fokus darauf, die Sicherheitsmechanismen möglichst effizient zu gestalten und die Kommunikation robust gegen Angriffe zu machen. Dies erreichen wir insbesondere vielfach durch probabilistische Maßnahmen.

## 1 Fahrzeug-Fahrzeug-Kommunikation

Die Kommunikation zwischen Fahrzeugen (so genannte Inter-vehicle communication) eröffnet eine Reihe neuer Anwendungsmöglichkeiten, um den Straßenverkehr in Zukunft sicherer, effizienter und komfortabler zu machen. Vorrangig arbeiten Fahrzeughersteller und Forschungseinrichtungen an Safety-Anwendungen, bei denen sich Fahrzeuge zum Beispiel gegenseitig vor Gefahrenstellen warnen können. Dies zeigt beispielhaft Abbildung 1. In einer Gefahrensituation, wie bei einem liegengebliebenen Fahrzeug oder bei einem Unfall, senden betroffene Fahrzeuge eine entsprechende Nachricht aus. Durch Weiterverteilung unter den Fahrzeugen in der Umgebung können herannahende Verkehrsteilnehmer rechtzeitig vor der Gefahr gewarnt werden. So können sich Fahrer frühzeitig auf die Situation einstellen, mit Vorsicht weiterfahren und dadurch Unfälle vermeiden.

Neben der Verbesserung der Verkehrssicherheit sind aber auch Anwendungen zur Erhöhung der Verkehrseffizienz denkbar. Beispielsweise wird an Assistenzfunktionen gearbeitet, die dem Fahrer fortlaufend die optimale Geschwindigkeit vorschlagen, um sich möglichst effizient durch ein städtisches Straßennetz zu bewegen.

Realisiert werden die Anwendungen durch drahtlose Ad-Hoc-Kommunikation, also spontaner Vernetzung von Fahrzeugen untereinander. Als Kommunikationsstandard wird voraussichtlich IEEE 802.11p [IEE] zum Einsatz kommen, eine Variante des verbreiteten WLAN-Standards. Für einige der geplanten Anwendungen reicht eine lokale Verbreitung

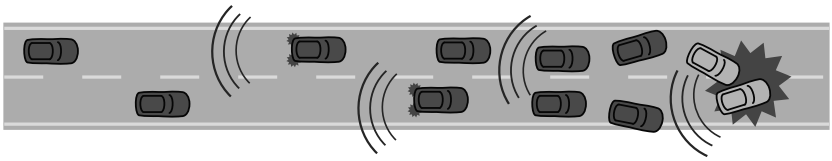

Abbildung 1: Beispielszenario auf einer Autobahn: Unfallfahrzeuge und stark bremsende Fahrzeuge senden Meldungen aus, die von anderen Fahrzeugen wiederholt und weitergeleitet werden. Dadurch können herannahende Fahrzeuge frühzeitig reagieren.

der Informationen an Fahrzeuge in direkter Funkreichweite aus. Andere Anwendungen erfordern jedoch eine Informationsweitergabe über größere Gebiete. Hierfür kommen verschiedene Weiterleitungsverfahren zum Einsatz, bei denen Informationen von Fahrzeug zu Fahrzeug weitergegeben werden. Eine häufige Kommunikationsform ist der so genannte Geobroadcast, kurz Geocast, bei dem Nachrichten innerhalb einer definierten, geographischen Zielregion per Multi-Hop-Verfahren verteilt werden [CMTLES05].

## 2 Sicherheits- und Privacy-Problematik

Die zumeist dezentrale Ad-Hoc-Kommunikation bietet allerdings auch viele Möglichkeiten zum gezielten Missbrauch durch Manipulation, Störung und Abhören. Ohne Gegenmaßnahmen könnte die Verkehrssicherheit durch mutwillige Eingriffe im schlimmsten Fall sogar gefährdet statt verbessert werden. Beispielsweise könnten widersprüchliche, gefälschte Nachrichten Fahrer verunsichern oder ablenken und dadurch die Nutzerakzeptanz deutlich schmälern. Aktive Fahrerassistenzfunktionen könnten durch Manipulation schwerwiegend gestört werden. Gleichermaßen problematisch ist das Abhören der Nachrichten, wenn diese einen gleichbleibenden Identifikator des Fahrzeugs beinhalten. Durch Kombinieren mitgehörter Nachrichten auf der Basis des Identifikators könnten Mithörer, entsprechend verteilte Präsenz vorausgesetzt, im schlimmsten Fall Bewegungsprofile von Fahrzeugen erstellen.

Die Einführung der Fahrzeug-Fahrzeug-Kommunikation ohne Berücksichtigung der Sicherheit gegenüber gezielten Angriffen ist daher nicht denkbar. Die Absicherung kann in verschiedene Bereiche aufgeteilt werden. Schwerpunkte bilden die Verlässlichkeit durch Authentisierung der Nachrichten, Absicherung der Kommunikationsmechanismen, Schutz gegen Denial-of-Service-Angriffe und der Schutz der Privatsphäre der Fahrzeuglenker bzw. -besitzer. Weitere Sicherheitszeile sind die Datenkonsistenz, der Schutz von Fahrzeuginternen Systemen vor Eingriffen über die Luftschnittstelle und die Absicherung der Fahrzeug-Sensorik.

## 3 Sichere Kommunikation

Obwohl letztendlich alle angesprochenen Bereiche bearbeitet werden müssen, um Fahrzeug-Fahrzeug-Kommunikation als Ganzes sicher zu machen, ist doch die Absicherung der Kommunikationsmechanismen der zentrale Aspekt. Ohne robuste und fehlertolerante Kommunikation als Kern des Systems lässt sich der Nutzen durch mutwillige Eingriffe leicht aufheben und es lassen sich widersprüchliche und gefälschte Informationen verteilen. Die Arbeit konzentriert sich deshalb darauf, die Sicherheit der verwendeten Kommunikationsverfahren zu untersuchen und geeignete Sicherheitsmechanismen zu entwickeln.

Dies ist insbesondere notwendig, weil sowohl die Anwendungen als auch die Ad-Hoc-Vernetzung sowie die hohe Mobilität der Fahrzeuge spezifische Kommunikationsverfahren benötigen. Für manche Anwendungen reicht aus, Nachrichten periodisch per Broadcast an alle Empfänger in Übertragungsreichweite zu versenden. Andere dagegen benötigen zwar keine periodische Aktivität, dafür aber die Verbreitung der Information in einem größeren Zielbereich über Multi-Hop Broadcast-Verfahren. Zudem steht nach aktuellem Stand nicht fest, welche Ansätze letztendlich zum Einsatz kommen werden. Der erste Schritt dieser Arbeit besteht deswegen darin, Anwendungen, typische Eigenschaften von Fahrzeug-Fahrzeug-Netzwerken und entsprechend beeinflussende Faktoren vorzustellen und zu charakterisieren. Dazu zählen insbesondere hohe Mobilität der Teilnehmer, typische Bewegungsmuster sowie Betrachtungen von Fahrzeugdichte, Fahrzeugausstattung und Netzwerkdimension. Diese Klassifikation bildet die Grundlage für eine Aufstellung charakteristischer Kommunikationsmuster, mit denen die meisten Anwendungen umgesetzt werden können und die den Netzwerkeigenschaften gerecht werden. Aufgrund der Anpassung an die typischen Eigenschaften von Fahrzeug-Fahrzeug-Netzen unterscheiden sich die Kommunikationsmuster signifikant von bisher in anderen Formen dynamischer Netze betrachteten Kommunikationsformen.

### 3.1 Kommunikationsmuster

Insgesamt identifizieren wir fünf relevante Kommunikationsmuster für Fahrzeug-Fahrzeug-Netze [ESFKTLMW08]: Beaconing, geographisches Routing, Geocast, Kontext-adaptive Verteilung und Aggregation (siehe Tabelle 1).

Als Kern der Arbeit führen wir für jedes der relevanten Kommunikationsmuster eine Analyse und Quantifizierung der Verwundbarkeit durch, basierend auf einem übergreifenden Analyseschema und einem gemeinsamen Angreifermodell. Insbesondere für Angriffe mit schwerwiegenden Auswirkungen erarbeiten wir speziell geeignete Sicherheitsmechanismen und evaluieren ihre Wirksamkeit. Sowohl für die Verwundbarkeit als auch den Entwurf von Sicherheitsmechanismen erweisen sich vor allem wiederum die Netzwerkcharakteristika sowie der automobile Anwendungsbereich als maßgebliche Einflussfaktoren.

Zur Quantifizierung von Auswirkungen eines Angriffs sowie zur Messung der Wirksamkeit und der Effizienz von Sicherheitsmechanismen verwenden wir eigens entwickelte Simulationswerkzeuge, die Straßenverkehrsszenarien, unterschiedliche Modelle von Kom-

| | |
|---|---|
| Beaconing | Periodischer (ca. 1–10 Hz) Single-Hop Broadcast von Statusdaten. |
| Geographisches bzw. positionbasiertes Routing | Unicast-Routing von Daten zu einem geographisch definierten Ziel, unter der Nutzung der Position einzelner (Zwischen-) Stationen. |
| Geocast | Multi-Hop Broadcast zur Verteilung einer Information in einer Zielregion. |
| Kontext-adaptive Informationsverteilung | Graduelle Verteilung, zeitliche Aufrechterhaltung einer Information, abhängig vom Kontext. |
| Aggregation | Graduelle Zusammenfassung von zueinander passenden Einzelinformationen zu Aggregaten mit höherwertiger Information, kontinuierliche Verbreitung der wichtigsten Informationen. |

Tabelle 1: Kommunikationsmuster in Fahrzeug-Fahrzeug-Netzen.

munikationsverfahren, Angriffen und Sicherheitsmechanismen hinreichend realistisch umsetzen.

### 3.2 Grundlegende Sicherheitsmechanismen

Bei der Untersuchung der Kommunikationsarten hat sich zunächst gezeigt, dass einige Sicherheitsmechanismen für alle Kommunikationsmuster notwendig sind, um eine grundlegende Sicherheit zu gewährleisten. Dazu zählt zum einen die Authentisierung und Integritätssicherung von Nachrichten mittels digitaler Signaturen und zum anderen der Schutz vor Replay-Angriffen. Das in der Arbeit vorgestellte Authentisierungsverfahren beruht auf dem im Projekt SEVECOM benutzten PKI-Ansatz, das den Einsatz von pseudonymisierten Zertifikaten zum Schutz der Privatsphäre vorsieht. Die Idee ist hier, Pseudonyme in gewissen zeitlichen Abständen zu wechseln und so die Erstellung von Bewegungsprofilen durch die Verknüpfung von Nachrichten über ein permanentes Zertifikat zu verhindern. Besonderheiten des entwickelten Identitätsmanagement-Konzepts sind unter anderem die Nutzung effizienter Kryptographieverfahren, Ausbalancierung des Tradeoffs zwischen Zertifikatslaufzeit und Revocation und die Gewährleistung der Privatsphäre von PKWs. Dazu werden Pseudonym-Zertifikate ausgegeben und von Fahrzeugen regelmäßig gewechselt [PBH+08]. Als Erweiterung dazu führt das in der Dissertation vorgestellte Verfahren ein spezielles Schema mit überlappenden und verschieden langen Zertifikatslaufzeiten ein, durch das Sybil-Angriffe erschwert werden und mit dem ein Fahrzeug Pseudonyme flexibler „nachfüllen“ kann. Dadurch bleibt beispielsweise die Kommunikation funktionsfähig, sollte ein Fahrzeug in seltenen Fällen keine Gelegenheit haben, gültige Pseudonyme nachzuladen, obwohl deren Gültigkeit ausgelaufen ist. Als weiteren, für alle Kommunikationsmuster gleichsam nutzbaren Schutzmechanismus gegen Replay-Angriffe schlagen wir „Geotimestamps“ vor. Neben einem Zeitstempel mit hinreichender Genauigkeit enthalten Geotimestamps auch den Absender-Ort sowie Paket-Sequenznummern.

Durch diese Daten kann man sowohl zeitlich späteres Wiedereinspielen als auch Tunneling von Daten an einen entfernten Ort erkennen.

Basierend auf den grundlegenden Sicherheitsmechanismen entwickeln wir dann speziell auf die einzelnen Kommunikationsmuster zugeschnittene Mechanismen.

### 3.3 Sicheres und effizientes Beaconing

Beaconing ist durch periodische Aussenden von MAC-Layer Broadcasts dazu vorgesehen, den eigenen Status mit Position, Geschwindigkeit, Richtung etc. an andere Fahrzeuge in Funkreichweite zu übertragen und dadurch zu ermöglichen, dass jeder Empfänger eine kontinuierliche Übersicht über das Geschehen in der lokalen Umgebung erhält. Auf der Basis des Beaconings können verschiedene Anwendungen aufbauen, beispielsweise die Warnung vor Kollisionen durch Spurwechsel oder eine Kreuzungsassistenzfunktion. Die systematische Angriffsanalyse zeigt, dass Beaconing durch die generelle Authentisierung von Nachrichten und den Replay-Schutz bereits hinreichend geschützt wird. Lediglich die Periodizität könnte als Angriffsvektor dienen, weil sich der Berechnungsaufwand zur Erzeugung und Verifikation digitaler Signaturen bis zur Überforderung der Verarbeitungshardware erhöhen ließe. Ein weiteres Problem ist, dass die Übertragung von Zertifikaten und Signaturen in jedem Beacon-Paket zusätzlich zu den Nutzdaten signifikant Kanalkapazität erfordert. Dieses Problem greift die Arbeit auf und entwickelt mehrere Verfahren zur Verbesserung der Effizienz, basierend auf der Idee, bestimmte Operationen wie Signaturprüfungen oder Zertifikatsübertragungen selektiv auszulassen, ohne jedoch die erzielte Sicherheit des Systems signifikant zu beeinflussen [ESFK10]. Beispielsweise können Zertifikate eingespart werden, wenn sich die lokale Topologie nicht ändert – in diesem Fall haben bereits alle Nachbarn ihre Zertifikate mit vorhergehenden Beacon-Paketen ausgetauscht. Effektiv bedeutet dies, dass ein Fahrzeug nur noch dann ein Zertifikat an ein Beacon-Paket anhängt, wenn in der Zwischenzeit seit seinem letzten gesendeten Beacon neue Nachbarn entdeckt wurden. Signaturverifikationen lassen sich ebenfalls auslassen, wenn durch andere Informationen mit einer gewissen Wahrscheinlichkeit von einem korrekten Beacon ausgegangen werden kann. Ein möglicher Ansatz hierzu ist, die Positionsangabe in Beacons zu verwenden, um zukünftige Positionen eines Knotens vorherzusagen, und die Abweichung der tatsächlichen Position von der geschätzten Position als Indikator für die Prüfwahrscheinlichkeit zu verwenden.

Die Auswertung zeigt, dass in beiden Fällen signifikant Berechnungs- und Übertragungsaufwand eingespart werden kann. Abbildung 2 stellt die Ergebnisse von Simulationen der Nachbar-basierten Zertifikatstrategie in mehreren Szenarien dar. Insbesondere bei hoher Nachrichtenfrequenz, wenn Kanalkapazität per se knapp ist, konnten bis zu $95\%$ der Beacons ohne Zertifikat versandt werden. Allerdings ergibt sich auch der Nachteil, dass in ungünstigen Fällen ein Zertifikat nicht vorliegt, oder eine gefälschte Signatur aufgrund der Auslassung der Verifikation nicht erkannt wird. Aber auch hier erweist sich das Verfahren als sehr robust – diese Fälle kamen in der Simulation nur in geringem Ausmaß vor (weniger als $2\,\%$).

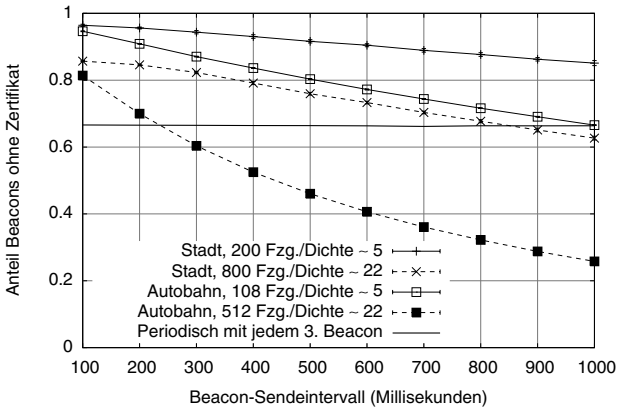


Abbildung 2: Prozentsatz der Beacon-Pakete, die kein Zertifikat beinhalten, wenn das Nachbarbasierte Schema eingesetzt wird. Zum Vergleich mehrere Szenarien und der Fall, dass Zertifikate periodisch angehängt werden.

### 3.4 Sicheres Georouting

Bei geographischem Routing werden Pakete jeweils von einem Knoten zum nächsten zu einer Zielposition hin weitergeleitet. Die Logik des Greedy-Schemas sieht vor, dass ein Knoten weiterzuleitende Pakete demjenigen seiner Nachbarn per Unicast überträgt, der von allen die geringste euklidische Distanz zur Zielposition aufweist. Bei der Angriffsanalyse des geographischen Routings erweist sich vor allem ein Angriff als kritisch, der es erlaubt, Pakete zum Angreifer umzuleiten, indem dieser seine eigene Position falsch angibt. In Szenarien mit langen Straßensegmenten wie Autobahnen kann es durch gezielte Wahl der gefälschten, eigenen Position sogar gelingen, jeglichen auf geographischem Routing basierenden Datenverkehr zum Angreifer umzuleiten.

Als Schutz gegen die Positionsfälschung entwickeln wir ein dezentrales, heuristisches Positionsverifikationsverfahren, das die Vertrauenswürdigkeit von Positionsangaben benachbarter Knoten ermittelt. Die Idee ist, physikalische Grenzen wie die Reichweite der Funktechnologie, die Geschwindigkeit von Fahrzeugen, Korrelation von Nachbarschaftsbeziehungen etc. mit der Positionsangabe eines Senders abzugleichen.

Beispielsweise kann ein Knoten bei Empfang einer Nachricht die Distanz $\Delta p$ zwischen eigener Position und der von einem anderen Fahrzeug angegebenen Position berechnen. Ist $\Delta p$ größer als die Funkreichweite, erscheint die Position des anderen Fahrzeugs unglaubwürdig. Aus mehreren solchen unscharfen Parametern berechnet das Verfahren fortlaufend einen Wert, der die Vertrauenswürdigkeit der Positionsangabe anderer Knoten darstellt.

Fälscht nun ein Knoten seine Position mit deutlicher Abweichung zur realen Position – was für erfolgreiches Umleiten nötig wäre – so wird dies mit hoher Wahrscheinlichkeit zu einem geringen Vertrauen in dessen Position führen. Knoten mit geringer Vertrauenswürdigkeit wiederum werden bei der Auswahl der potentiell weiterleitenden Nachbarn nicht berücksichtigt. Angreifer werden so lokal von der Kommunikation ausgeschlossen.

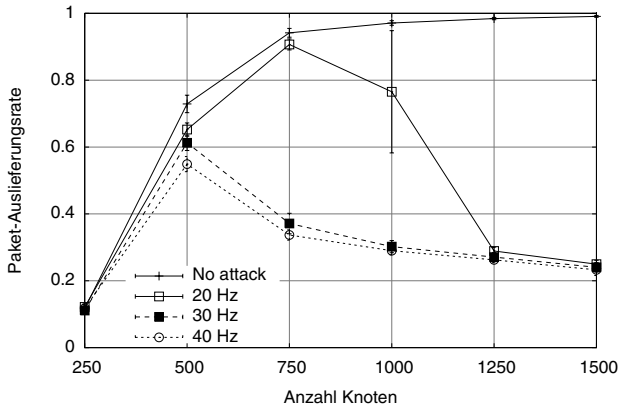


Abbildung 3: Fluten mit Geocast Nachrichten erzeugt je nach Knotendichte und Frequenz neuer Nachrichten sehr schnell eine Sättigung auf dem Kanal. Im dargstellten Szenario wurde nur ein einzelner Angreifer angenommen, der die maximal mögliche Zielregionsgröße einstellt.

Die Neuartigkeit dieser Positionsprüfung liegt darin, dass das vorgestellte Verfahren ohne Messungen von Signallaufzeiten und ohne Infrastruktur auskommt, die üblicherweise für Positionierung nötig sind. Die Positionsprüfung ist zwar probabilistisch, aber erkennt trotzdem sehr zuverlässig, wenn ein Knoten eine falsche Position angibt [TLESFKCM06, TLESFK06].

### 3.5 Sicherer Geocast

Ein weiteres klassisches Kommunikationsmuster für Fahrzeug-Fahrzeug-Netze, Geocast, flutet Nachrichten im Netz, beschränkt durch eine geographisch definierte Zielregion. Besonders deutliche Auswirkungen auf Geocast haben Angriffe basierend auf selektivem bzw. reaktivem Jamming sowie das massenhafte Erzeugen und Versenden von Nachrichten. Die Basis des selektiven Jammings ist, Übertragungen anderer Knoten zu detektieren und erst dann ein Störsignal zu senden. Dies trifft das auf MAC-Layer-Broadcasts basierende Geocast besonders, da diese Broadcast-Frames im Gegensatz zu Unicast-Frames nicht bestätigt und daher nicht wiederholt werden. Kritisch ist dies im Autobahnszenario, weil durch die Beschränkung der Netztopologie auf den räumlich schmalen Korridor der Straße keine alternativen Verteilungspfade verfügbar sind.

Ein weiterer Angriff basiert darauf, das Netz mit Nachrichten zu überschwemmen. Dieses massive Fluten mit Nachrichten trifft beliebige Topologien und stört die normale Kommunikation in größeren Regionen durch Überlastung des Funkkanals. Wie Abbildung 3 zeigt, reicht eine Nachrichtenfrequenz von 20 Hz, kombiniert mit großer Zielregion, um die Nachrichtenverteilung bei höherer Knotendichte kollabieren zu lassen. Dagegen wirkt der vorgeschlagene Ansatz einer Lastmetrik, in die für Geocast relevante Werte wie Zielregionsgröße, Frequenz und Nachrichtengröße einfließen, und die durch ein adaptives

Schwellwertverfahren kontrolliert wird. Gegen selektives Jamming nutzen wir die Möglichkeit impliziter Bestätigungen durch weiterleitende Knoten. Kann ein Knoten in einer kurzen Zeitspanne nach der eigenen Weiterleitung einer Nachricht keine Weiterleitung derselben Nachricht durch andere Knoten feststellen, so wiederholt er die Nachricht nach einem definierten Schema. Dadurch werden Stellen mit stationären Angreifern durch die Fortbewegung der Fahrzeuge überbrückt.

### 3.6 Sichere kontextadaptive Nachrichtenverteilung

Obwohl Geocast für viele Anwendungen in Fahrzeug-Fahrzeug-Netzen geeignet ist, verlangen manche Anwendungen weitere Mechanismen: Nachrichten sollen über längere Zeit im Netz kursieren, um neu hinzukommende Fahrzeuge ebenfalls zu informieren, oder der Sender kann zum Zeitpunkt der Erstellung keine Zielregion definieren. Als Lösung wurde kontextadaptive Nachrichtenverteilung vorgeschlagen. Hierzu werden Nachrichten zwischengespeichert, ihre Relevanz im aktuellen Umfeld kontinuierlich bewertet und durch ein Relevanz-gesteuertes Medienzugriffsverfahren jeweils die Nachricht mit der größten Bedeutung weiterverbreitet [TKCJASE+06]. Durch die dezentrale Bewertung zeigt sich das Verfahren bereits robust gegen gefälschte Parameter wie Position oder Zeitpunkt des beschriebenen Ereignisses. Ebenso kann ein massenhaftes Fluten keine Überlast erzeugen, da die Last durch die Auswahl der wichtigsten Nachricht zu jedem Zeitpunkt geregelt ist. Allerdings kann ein Angreifer normale Nachrichten aus den begrenzten Speichern anderer Knoten verdrängen. Das hat zur Folge, dass einige Knoten sehr stark beeinflusst werden und der Informationsfluss entlang längerer Straßensegmente unterbrochen werden kann [ESMKFKMW08]. Als Gegenmaßnahme führen wir hier passend zum Schema den Sicherheitskontext ein. Basierend auf Beobachtungen des Knotenverhaltens und der Nachrichtenkonsistenz definieren wir Kontextparameter, die zusätzlich Einfluss auf die Relevanz von Nachrichten haben. Dadurch werden die Angreifernachrichten abgewertet und die Auswirkungen der Angriffe weitgehend entschärft.

### 3.7 Sichere kollaborative Aggregation

Insbesondere in Situationen wie Staus, bei denen die Fahrzeugdichte hoch ist, besteht weiteres Optimierungspotential bei der Verbreitung von Informationen. Durch Zusammenfassen ähnlicher Nachrichten kann signifikant Bandbreite bei der Weiterverbreitung gespart werden. So entsteht ein gradueller Aggregationsprozess, dessen Nachrichten einen höheren Informationsgehalt haben, beispielsweise zum gleichmäßigen Geschwindigkeitsprofil eines ganzen Straßenabschnitts [SDBBESFK09].

Angreifer können diese erhöhte Bedeutung von aggregierten Nachrichten ausnutzen und direkt solche Nachrichten mit größerer Aussagekraft erzeugen. Beispielsweise könnte ein Angreifer mit einem einzigen Paket einen nicht existierenden Stau auf einem Straßenabschnitt vorgeben und andere Verkehrsteilnehmer zum Verlassen der Strecke veranlas-

sen. Die Sicherheitslösung muss daher den Aggregationsprozess für Empfänger eines Aggregats nachvollziehbar machen, damit Fahrzeuge die Richtigkeit von Aggregaten prüfen können. Dies erreichen wir durch Hinzufügen signierter Einzelwerte zum Aggregat. Einzelwerte sind nicht-aggregierte, atomare Informationen von einzelnen Fahrzeugen, die vom Sender digital signiert wurden. Die Einzelwerte sollen die Information des Aggregats möglichst optimal stützen. Durch die semantische Verknüpfung zwischen Aggregat und ausgewählten Einzelwerten kann ein Fahrzeug die Vertrauenswürdigkeit eines Aggregats einschätzen und sowohl bei der Aggregation mit anderen Informationen als auch bei der Weiterverbreitung berücksichtigen. Anhand des Beispiels der Verbreitung von Geschwindigkeitsdaten zeigen wir, dass die Lösung sowohl das künstliche Erzeugen eines Staus mit geringem Geschwindigkeitsdurchschnitt als auch die Unterdrückung einer existierenden Stauung erfolgreich detektieren kann [SDESFK+10].

## 4 Zusammenfassung

Fahrzeug-Fahrzeug-Kommunikation ermöglicht eine große Bandbreite neuer Anwendungen zur Verbesserung der Verkehrssicherheit und der Effizienz im Straßenverkehr. Die Kommunikation muss jedoch auch zuverlässig funktionieren und soll nicht missbraucht werden können. Die Arbeit greift dieses Thema auf. Zunächst ist notwendig, charakteristische Kommunikationsmuster zu identifizieren. Die darauf aufbauende Sicherheitsanalyse zeigt deutlich die jeweiligen Schwächen der Kommunikationsformen. Für jedes der Kommunikationsmuster werden daher Sicherheitsmechanismen entwickelt, die auf Effizienz und Robustheit ausgelegt sind. Es geht darum, in erster Linie die Kommunikation auch unter Angriffen und mit möglichst geringem technischen Aufwand aufrecht zu erhalten. Dies erreichen wir häufig durch eine Abkehr von der klassischen Definition starker Sicherheit hin zu probabilistischen Verfahren. Wie die quantitative Evaluation zeigt, gelingt es mit den vorgeschlagenen Verfahren, Sicherheitsmechanismen für Fahrzeugkommunikation effizienter zu machen, viele Angriffe mit hoher Wahrscheinlichkeit zu erkennen und zu verhindern, oder zumindest ihre Auswirkungen signifikant zu reduzieren.

## Literatur

[CMTLES05] Christian Maihöfer, Tim Leinmüller, und Elmar Schoch. Abiding Geocast: Time–Stable Geocast for Ad Hoc Networks. In *VANET '05: Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks*, Seiten 20–29, New York, NY, USA, 2005. ACM Press.

[ESFK10] Elmar Schoch und Frank Kargl. On the Efficiency of Secure Beaconing in VANETs. In *Third ACM Conference on Wireless Network Security (WiSec)*, Marz 2010.

[ESFKTLMW08] Elmar Schoch, Frank Kargl, Tim Leinmüller und Michael Weber. Communication Patterns in VANETs. *IEEE Communications Magazine*, 46(11), November 2008.

[ESMKFKMW08] Elmar Schoch, Moritz Keppler, Frank Kargl und Michael Weber. On the Security of Context-Adaptive Information Dissemination. *Security and Communications Networks*, 1(3):205–218, Mai 2008.

[IEE] IEEE 802.11p. Wireless Access for Vehicular Environments (WAVE) – Draft standard.

[PBH+08] Panos Papadimitratos, Levente Buttyán, Tamas Holczer, Elmar Schoch, Julien Freudiger, Maxim Raya, Zhendong Ma, Frank Kargl, Antonio Kung und Jean-Pierre Hubaux. Secure Vehicular Communication Systems: Design and Architecture. *IEEE Communication Magazine*, 46(11), November 2008.

[SDBBESFK09] Stefan Dietzel, Boto Bako, Elmar Schoch und Frank Kargl. A Fuzzy Logic based Approach for Structure-free Aggregation in Vehicular Ad-Hoc Networks. In *The Sixth ACM International Workshop on VehiculAr Inter-NETworking (VANET 2009)*, September 2009.

[SDESFK+10] Stefan Dietzel, Elmar Schoch, Frank Kargl, Bastian Könings und Michael Weber. Resilient Secure Aggregation for Vehicular Networks. *IEEE Network*, 24(1):26 – 31, Januar 2010.

[TKCJASE+06] Timo Kosch, Christian J. Adler, Stephan Eichler, Christoph Schroth und Markus Strassberger. The Scalability Problem of Vehicular Ad Hoc Networks and How to Solve it. *IEEE Wireless Communications*, 13(5):22–28, Oktober 2006.

[TLESFK06] Tim Leinmüller, Elmar Schoch und Frank Kargl. Position Verification Approaches for Vehicular Ad Hoc Networks. *IEEE Wireless Communication Magazine*, Oktober 2006.

[TLESFKCM06] Tim Leinmüller, Elmar Schoch, Frank Kargl und Christian Maihöfer. Improved Security in Geographic Ad Hoc Routing through Autonomous Position Verification. In *The Third ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2006) - in conjunction with MobiCom 2006*, Seiten 57–66, September 2006. isbn: 1-59593-540-1.

**Elmar Schoch** arbeitet seit mehreren Jahren im Bereich Fahrzeug-Fahrzeug-Kommunikation. Während des Studiums an der Universität Ulm war er für die Daimler Forschung in frühen Projekten wie FleetNet und Network-on-wheels (NOW) aktiv, insbesondere zu „Abiding Geocast“. Nach der Diplomarbeit bei Daimler kehrte er 2005 zur Promotion zurück an die Universität Ulm, eingebunden in das Projekt SEVECOM. Dieses EU-geförderte Forschungsprojekt widmete sich erstmalig speziell dem Thema Sicherheit und Privatsphäre in Fahrzeug-Fahrzeug-Netzen. Parallel dazu arbeitete er mit Kollegen aus der Automobilindustrie im Car-to-car Communication Consortium an Sicherheitsmechanismen der zukünftigen Vernetzung zwischen Fahrzeugen. In 2009 schloss er seine Promotion mit Auszeichnung ab, die sich mit der Sicherheit der Kommunikationsmechanismen in Fahrzeug-Fahrzeug-Netzen gegenüber Angriffen befasste. Aktuell führt er das Thema im industriellen Umfeld in der Konzernforschung der Volkswagen AG und bei der Audi AG fort. Weitere Forschungsinteressen sind Ubiquitous Computing, intelligente Mobilität, Simulation, sowie neue Ansätze für Security, Privacy und Trust in zukünftigen, vernetzten Systemen.