Aktuelle Trends in der sicheren Fahrzeug-Fahrzeug Kommunikation

Frank Kargl, Elmar Schoch, Zhendong Ma
Universität Ulm, Institut für Medieninformatik
{*vorname.nachname*}@uni-ulm.de

***Zusammenfassung*—Dieser Beitrag zeigt aktuelle Trends der Informationsverteilung in Fahrzeug-Fahrzeug Netzen und analysiert Auswirkungen auf und mögliche Lösungsansätze für Sicherheit und Schutz der Privatsphäre.**

I. Einleitung

Seit einigen Jahren wird das Thema der Fahrzeug-Fahrzeug-Kommunikation vor allem in den USA, in Europa und in Japan intensiv untersucht. Ausgehend von initialen Forschungsprojekten der ersten Generation wie Fleetnet oder VSC wurden einerseits weitere Forschungsaktivitäten gestartet (z.B. Network-on-Wheels, VII, CVIS, Safespot), andererseits arbeiten verschiedene Organisationen bereits an der Standardisierung von Kommunikationsmechanismen und Protokollen. Hier sind vor allem die Aktivitäten der IEEE (802.11p, 1609.x), ISO-CALM und das Car-2-Car Communication Consortium zu nennen.

Im Rahmen dieser Aktivitäten wird bereits die Sicherheit und der Datenschutz zukünftiger Systeme untersucht. In den USA mündete dies in den vorläufigen IEEE 1609.2 Standard, in Europa ist in diesem Bereich vor allem das Projekt Secure Vehicle Communication (SeVeCom) aktiv.

All diesen Standardisierungsbemühungen und Projekten ist zu eigen, dass sie eine relativ abgegrenzte Menge von Kommunikationsformen betrachten. Dies sind vor allem

1) **Beaconing:** direktes und periodisches Senden von Broadcast-Nachrichten an alle Nachbarn in Reichweite der drahtlosen Kommunikationstechnologie.
2) **Flooding und Geocast:** Verteilung[1] von Broadcast Nachrichten, wobei Empfängerknoten Nachrichten auch weiterleiten. Um die Weiterleitung zu begrenzen, kommen z.B. Time-to-Life (TTL) Zähler oder im Falle von Geocast [1] die Angabe eines geographischen Verbreitungsgebiets zum Einsatz.
3) **Positionsbasiertes Routing:** Im Gegensatz zu topologie-basiertem Routing, wie es oft in MANETs eingesetzt wird, hat sich bei Fahrzeug-Fahrzeug Netzen positionsbasiertes Routing als besser geeignet erwiesen [2].

Dies sind auch die Mechanismen, deren Sicherheits- und Datenschutzaspekte am genauesten untersucht wurden (z.B. in [3], [4]). In jüngerer Zeit gibt es jedoch Hinweise und Aktivitäten, die darauf hindeuten, dass diese einfachen Kommunikationsformen manche Anwendungen nicht ausreichend unterstützten.

Deshalb werden aktuell zusätzliche Kommunikationsverfahren untersucht, welche im folgenden Abschnitt kurz vorgestellt werden sollen. Anschließend wird diskutiert, inwiefern diese anderen Formen der Kommunikation auch geänderte Anforderungen an ein Sicherheitssystem stellen.

[1] gegebenenfalls auch periodisch

II. Fortgeschrittene Kommunikationsmuster

Ein Ansatz, der in jüngerer Zeit untersucht wird, ist die *Effizienzsteigerung bei Flooding und Geocast*. Abhängig von Netzwerkparametern wie Knotendichte oder Topologie muss gegebenenfalls nicht jeder Knoten ein empfangenes Packet erneuten broadcasten. Statt dessen verwenden die verschiedenen Varianten des sog. Gossiping [5] eine geringere Weiterleitungswahrscheinlichkeit, die entweder statisch oder anhand von Netzwerkparametern festgelegt wird. Damit lassen sich signifikante Effizienzsteigerungen erzielen.

Bei der *Context-adaptive Message Dissemination* [6] geht es ebenfalls um das Verteilen von Paketen bzw. Informationen. Hier speichert jeder Empfänger von Daten diese zunächst lokal und entscheidet dann anhand einer Relevanzfunktion, welche Daten er im momentanen Kontext für besonders wichtig für seine Nachbarn hält und schickt diese priorisiert weiter. Parameter können Abstand zum Ursprung der Information, deren Alter, uvm. sein. Durch eine Anpassung der Wartezeiten im Medienzugriff kann darüber hinaus auch eine Priorisierung zwischen Knoten erreicht werden. *Context-adaptive Message Dissemination* sorgt vor allem dafür, dass bei einer gegebenen Netzwerkkapazität diese vor allem zur Weiterleitung der relevanten Informationen genutzt wird.

Aggregation geht noch einen Schritt weiter. Hier empfängt ein Fahrzeug Daten von seinen Nachbarn, z.B. über deren aktuelle Geschwindigkeit. Vor einer möglichen Weiterleitung werden diese Daten allerdings zunächst aggregiert, d.h. zusammengefasst. Dies kann sinnvoll sein, wenn z.B. bei einem Stau sehr viele Fahrzeuge gleiche oder ähnliche Informationen senden. Hier wird also die Menge der zu sendenden Information direkt reduziert und damit die Kommunikationslast reduziert.

III. Sicherheit bei fortgeschrittenen Kommunikationsmustern

Betrachtet man Gossipping, Context-adaptive Message Dissemination und Aggregation unter dem Aspekt von Sicherheit und Schutz der Privatsphäre, so stellt man fest, dass die Protokolle bereits eine gewisse Resistenz gegen Angriffe zeigen. Da es im Gegensatz zu vielen Routingprotokollen keine oder sehr wenig direkte Signalisierung zwischen den Fahrzeugen gibt, fallen viele Angriffsmöglichkeiten schlicht weg. Der Angreifer ist im Wesentlichen auf Denial-of-Service Angriffe oder das Verfälschen der Information beschränkt.

Damit versagen aber auch herkömmliche, auf Kryptographie-basierende Sicherheitsmechanismen[2]. Solche Mechanismen setzen vor allem auf einen Sender-basierten Schutz, bei dem der Sender einer Nachricht diese durch Signaturen vor Veränderungen oder durch Verschlüsselung vor Ausspähung schützt. Weiterhin gehen diese oft von einem statischen Paketinhalt aus, der unverändert oder mit wenigen Veränderungen im Header durch das Netzwerk verschickt wird. Während letzteres zumindest bei Gossiping noch zutrifft, kann die Information bei Context-adaptive Message Dissemination bereits beim Versenden neu in Pakete gepackt werden und beim Einsatz von Aggregationsverfahren geht die Einzelinformation vollkommen verloren.

Der Sender- und Paketzentrierte Ansatz muss deshalb durch einen Daten-orientierten Ansatz erweitert bzw. ersetzt werden. Hier kommen Mechanismen wie Konsistenzchecks zum Einsatz, welche die Plausibilität der Informationen und die Konsistenz der Informationen bei redundanter Verteilung oder mehrerer Informationsquellen prüfen. Vorhandene Sensoren wie RADAR oder LIDAR können für zusätzliche Konsistenzchecks genutzt werden.

Werden Inkonsistenzen erkannt, die auf einen Angriff hindeuten, so kommen reaktive Sicherheitsmechanismen zum Einsatz, die gefälschte Daten erkennen und verwerfen, die Verteilung durch Erhöhung der Redundanz robuster gegen Angriffe machen oder in anderer Weise auf den erkannten Angriff reagieren. Beispielsweise können Ratenkontrollmechanismen verhindern, dass einzelne Knoten das Netz mit Informationen fluten, um eine Überlastsituation zu erreichen.

Abbildung 1 zeigt die Auswirkungen eines Angriffs auf die kontext-adaptive Nachrichtenverteilung, wenn der Angreifer gefälschte Nachrichten mit hoher Rate absetzt. Anhand der Färbung kann man sehen, dass sich dadurch die Queues von Knoten in der Umgebung des Angreifers nach und nach mit gefälschten Nachrichten füllen. Der Angreifer ist also in der Lage, die reguläre Kommunikation in einer gewissen Umgebung sehr stark zu stören.

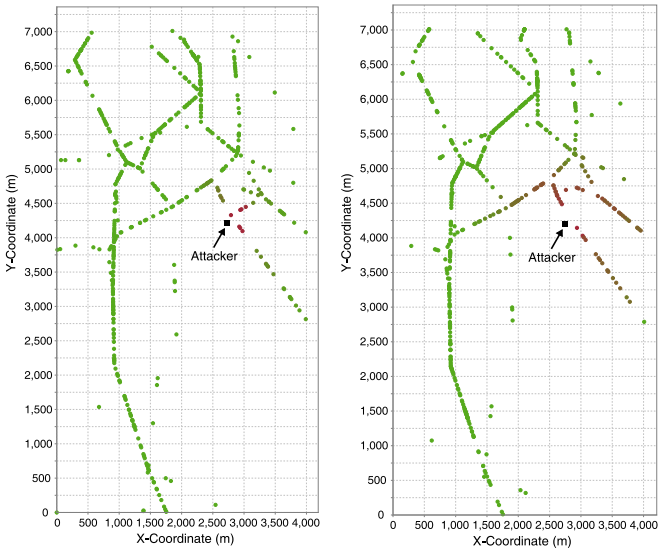

Abbildung 1. Verlauf eines Angriffs auf Context-adaptive message dissemination, bei dem der Angreifer gefälschte Nachrichten mit hoher Frequenz absetzt - Status der Queues nach 20s (links) und 50s (rechts)

IV. Zusammenfassung und Ausblick

Zusammenfassend lässt sich sagen, dass die genannten Kommunikationsformen erfolgreich die Effizienz der Fahrzeug-Fahrzeug Kommunikation verbessern und dabei die Anpassung an stark wechselnde Fahrzeugdichten ermöglichen.

Gleichzeitig zeigen unsere Untersuchungen, dass die Mechanismen per se bereits eine gewisse Sicherheit gegenüber Angriffen bieten. Zum Schutz gegen Angriffen können insbesondere Konsistenzprüfungen und Ratenkontrollmechanismen beitragen. Wir sind zur Zeit dabei, derartige Mechanismen zu entwerfen und zu evaluieren.

Literatur

[1] Christian Maihöfer, "A Survey Of Geocast Routing Protocols," *IEEE Communications Surveys*, vol. 6, no. 2, pp. 32–42, 2004.

[2] Holger Füssler, Martin Mauve, Hannes Hartenstein, Michael Käsemann, and Dieter Vollmer, "A Comparison of Routing Strategies for Vehicular Ad Hoc Networks," Department of Computer Science, University of Mannheim, Technical Report TR-3-2002, Jul. 2002.

[3] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in *VANET '07*. New York, NY, USA: ACM, September 2007, pp. 19–28.

[4] E. Schoch, F. Kargl, T. Leinmüller, and M. Weber, "Vulnerabilities of geocast message distribution," in *2nd IEEE Workshop on Automotive Networking and Applications (AutoNet 2007, in conj. with GlobeCom 2007)*, Washington, DC, USA, Nov. 2007.

[5] J. Luo, P. Eugster, and J. Hubaux, "Route driven gossip: Probabilistic reliable multicast in ad hoc networking," in *Infocom*, 2003.

[6] Markus Strassberger, Christian Adler, and Robert Eigner, "Situationsadaptive Verbreitung von Kontextinformationen in automobilen Ad-hoc-Netzen," *Praxis der Informationsverarbeitung und Kommunikation*, vol. 1, no. 29, pp. 43–49, Mar. 2006.

[2] wobei zur Verhinderung von Sybil-Angriffen nach wie vor eine Authentisierung gültiger Fahrzeuge notwendig ist.