Vorschlag für eine Sicherheitsinfrastruktur für Vehicular Ad Hoc Networks

Klaus Plößl, Hannes Federrath
Universität Regensburg
Klaus.Ploessl@wiwi.uni-regensburg.de

In diesem Papier wird eine Sicherheitsinfrastruktur für Vehicular Ad Hoc Networks (VANETs) vorgestellt, die durch Kombination einer Authentifizierung basierend auf asymmetrischer Kryptographie und eines darauf aufbauenden symmetrischen Verschlüsselungs- und Authentifizierungssystems besonders gut den Anforderungen eines VANETs angepasst ist. Die Sicherheitsinfrastruktur ermöglicht es, die Integrität und Authentizität aller Nachrichten im VANET zu sichern ohne dabei gravierende Performance-Einbußen oder Verletzungen der Privatsphäre hinnehmen zu müssen. Der Vorschlag basiert auf einer detaillierten Anforderungsanalyse und einigen grundsätzlichen Überlegungen zu Identitäten und Authentifizierung in VANETs.

1 Einleitung

Vehicular Ad Hoc Networks (VANETs) können als Untergruppe der in [MS02] definierten Mobile Ad Hoc Networks (MANETs) verstanden werden. Die Datenübertragung erfolgt drahtlos und jeder Teilnehmer (Knoten) muss Nachrichten anderer Knoten weiterleiten, um das Funktionieren des Netzes zu gewährleisten. Das charakterisierende Merkmal der VANETs ist, dass als Knoten nur Fahrzeuge wie PKWs, LKWs oder Busse angenommen werden. Die Bewegung der Knoten ist dadurch nicht beliebig, sondern folgt den vorhandenen Straßen und Verkehrsregeln und wird teilweise vom Verhalten der anderen Knoten beeinflusst. Durch die relativ fest vorgegebenen Bewegungsmöglichkeiten können an neuralgischen Punkten (wie z.B. viel befahrenen Straßen, gefährlichen Stellen usw.) stationäre Transmitter aufgestellt werden, die bestimmte Dienste übernehmen und Zugriff auf andere (stationäre) Netze vermitteln können (vgl. [RH05]). Fahrzeuge unterliegen auch in den Punkten Energieversorgung, verfügbarer Platz und vorhandene Rechenkapazität nicht den strikten Beschränkungen, die üblicherweise in MANETs angenommen werden [TC03]. Eher nachteilig sind die potentiell sehr hohen Geschwindigkeiten der Knoten (bis zu 250 km/h) und die große Ausdehnung von VANETs.

Hauptziel eines VANET ist die Erhöhung der Verkehrssicherheit. Dieses Ziel wird erreicht, indem lokal im Fahrzeug zur Verfügung stehende Telematikdaten z.B. über aktuelle Geschwindigkeit, Beschleunigung, Position usw. mit den anderen Fahrzeugen ausgetauscht werden und so in jedem Fahrzeug ein globaleres Bild der Verkehrssituation entsteht. Abnormale oder gefährliche Straßenverhältnisse wie Unfälle, Staus oder Glatteis können so frühzeitig erkannt werden und der Fahrer hat mehr Zeit, adäquat darauf zu reagieren. Neben diesem Austausch von Telematikdaten (und daraus resultierenden Warnungen) sollen auch Einsatzsignale und Anweisungen z.B. von Polizei oder Feuerwehr über das VANET verteilt werden, die unter anderem durch Beeinflussung der Ampelanlagen für freie Fahrt für die Einsatzfahrzeuge sorgen sollen. Neben diesen

Anwendungen, die die Verkehrssicherheit und das Verhalten der Teilnehmer direkt beeinflussen, sind auch viele Dienste geplant, die im Komfortbereich liegen, wie z.B. Location Based Services, Internetzugriff, Fernwartung des Fahrzeugs usw. (vgl. [PNM06]).

Diese drei Kategorien implizieren unterschiedliche Anforderungen an die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. Dennoch wird zum Erreichen der Schutzziele immer eine Sicherheitsinfrastruktur benötigt, die eine Vertrauensbasis schafft und den Einsatz von Kryptographie ermöglicht. Die Sicherheitsinfrastruktur umfasst also alle technischen und organisatorischen Maßnahmen und Einrichtungen, die zum Erreichen der Schutzziele benötigt werden. Im Folgenden werden Anforderungen an eine solche Sicherheitsinfrastruktur definiert (Kapitel 2) und grundsätzliche Fragen diskutiert (Kapitel 3). Darauf aufbauend wird in Kapitel 4 ein eigener Vorschlag präsentiert.

2 Anforderungen

In diesem Abschnitt werden die Anforderungen an eine Sicherheitsinfrastruktur für VANETs genauer erläutert. Falls nötig wird dabei nach den drei Anwendungskategorien „Telematiknachrichten und Warnungen“ (A1), „Alarmsignale und Anweisungen“ (A2) und „Komfort-Dienste“ (A3) unterschieden. Die Anforderungen sind in Tabelle 1 auf Seite 4 zusammengefasst.

2.1 Integrität

Die Sicherheitsinfrastruktur muss Mechanismen zur Verfügung stellen, die eine Veränderung der Nachrichten bei der Übertragung im VANET verhindern bzw. erkennbar machen (I1). Bösartige Zwischenstationen können somit weiterzuleitende Nachrichten nicht mehr unbemerkt verändern.

Für Nachrichten aus A2 muss der Empfänger zusätzlich die Identität bzw. die Autorisierung des Senders zum Versenden solcher Nachrichten eindeutig feststellen können (I2a), da der Empfänger solchen Nachrichten „blind“ Folge leisten muss. Im Gegensatz dazu sind bei Nachrichten aus A1 Plausibilitätsprüfungen mit Hilfe eigener Sensoren und Nachrichten anderer Verkehrsteilnehmer möglich, wodurch die eindeutige Identifizierung des Senders nicht unbedingt nötig ist. Um die Erstellung von Bewegungs- oder Dienstnutzungsprofilen zu erschweren, ist es hier sogar wünschenswert, die Identität des Senders in der Nachricht nicht preisgeben zu müssen (D1). Um ungestraftes Einspeisen falscher Informationen oder unberechtigte Dienstnutzung zu verhindern, sollte es allerdings auch für solche Nachrichten möglich sein, die Identität des Absenders – zumindest nachträglich – zweifelsfrei nachweisen zu können (I2b). Es müssen also auch die Schutzziele Zurechenbarkeit und Nichtabstreitbarkeit erreicht werden können. Anonyme Teilnahme am VANET sollte daher verhindert werden, pseudonyme Teilnahme ist wünschenswert.

Eine nachträgliche Aufdeckung der Identität darf dabei aber nur bei schwerwiegenden Verstößen (z.B. wiederholtes Versenden falscher Warnungen, die die Verkehrssicherheit gefährdeten) und unter genau definierten Bedingungen möglich sein. Eine automatisierte Überwachung oder Strafverfolgung – beispielsweise aufgrund der verschickten Telematikdaten – darf im Sinne der mehrseitigen Sicherheit nicht möglich sein (D2). Mehrseitige Sicherheit bedeutet, dass die Interessen aller Beteiligten berücksichtigt werden. Im konkreten Fall sind also die Interessen der Strafverfolgungsbehörden (möglichst jeden Verstoß gegen die Straßenverkehrsordnung mit möglichst wenig Aufwand zu verfolgen) den Interessen der Bürger (nicht verdachtsunabhängig überwacht und automatisiert bestraft zu werden) gegenüberzustellen.

Dass die innerhalb des Fahrzeugs von Sensoren erhobenen Daten korrekt sind, wird vorausgesetzt. Die Einbindung von korrekten Zeit- und Ortsangaben in die Nachrichten zum Schutz vor Replay- und Position-Spoofing-Angriffen wird ebenfalls vorausgesetzt. Diese Daten werden von anderer Infrastruktur wie beispielsweise Galileo [Eur03] bereitgestellt.

2.2 Vertraulichkeit

Die Anforderungen an die Vertraulichkeit unterscheiden sich stark zwischen den drei Anwendungskategorien. Während bei Alarmsignalen die Vertraulichkeit der Nutzdaten zu vernachlässigen ist, ist bei den unter Umständen kostenpflichtigen Komfort-Diensten Vertraulichkeit meist sehr wichtig, um eine unberechtigte Dienstnutzung bzw. unerwünschten Informationsgewinn in Zwischenknoten zu verhindern. Die Sicherheitsinfrastruktur muss also Mechanismen bieten, mit denen die Vertraulichkeit der Nutzdaten in verschiedenen Stufen (keine Vertraulichkeit, Vertraulichkeit vor Nicht-VANET-Teilnehmern, Vertraulichkeit vor allen nicht direkten Kommunikationspartnern) erreicht werden kann (V1).

Da unter Umständen schon das bloße Wissen über eine bestehende Kommunikationsbeziehung zwischen zwei Parteien unerwünschten Informationsgewinn mit sich bringen kann, sollten auch die Identitäten der Sender und Empfänger bestmöglich geschützt werden (D3), ohne allerdings die oben geforderte Zurechenbarkeit und Nichtabstreitbarkeit zu gefährden. Bezüglich der Vertraulichkeit der Nutzdaten gibt es keine direkten Abhängigkeiten zur Zurechenbarkeit und Inhaltsintegrität, sie kann also weitgehend unabhängig realisiert werden.

Neben den Anwendungs- und Verbindungsdaten müssen auch administrative Nachrichten, wie Nachrichten des Routingprotokolls oder Nachrichten zum Management verwendeter kryptographischer Schlüssel vor unbefugtem Abhören geschützt werden (V2). Auch die kryptographischen Schlüssel, die sich im Besitz der Teilnehmer oder auch zentraler Instanzen befinden, müssen vor unberechtigtem Zugriff geschützt werden. Allgemeiner formuliert ist auch die Sicherheitsinfrastruktur vor Angriffen zu schützen (V3).

2.3 Performance

Da viele Nachrichten im VANET der Erhöhung der Verkehrssicherheit dienen, hängen im Extremfall Menschenleben von der rechtzeitigen Verarbeitung der Nachrichten ab (Verfügbarkeit). Um aber die oben genannten Integritäts- und Vertraulichkeitsanforderungen zu erfüllen, müssen von den Rechnereinheiten der VANET-Teilnehmer zusätzliche kryptographische Operationen durchgeführt werden, die das Aufbereiten der Nachrichten zeitlich erheblich verlängern. Die Maßnahmen der Integritätssicherung vergrößern die Nachrichtenlänge. Um den gestellten Echtzeitanforderungen gerecht werden zu können, sollten die von der Sicherheitsinfrastruktur zur Verfügung gestellten Mechanismen also möglichst effizient im Bezug auf benötigte Rechenkapazität und Bandbreite sein (P1). Wünschenswert sind auch Maßnahmen, die Denial-of-Service (DoS) Angriffe verhindern oder zumindest erschweren und dadurch die Verfügbarkeit erhöhen.

2.4 Wirtschaftlichkeit und Akzeptanz

Aufbau und Betrieb der Sicherheitsinfrastruktur sind mit Kosten verbunden, die sich vor allem bei der Einführung von VANETs deutlich auf die Ausstattungsrate von Fahrzeugen mit VANET-Technologie und damit auf den Nutzwert dieses Netzes auswirken können. Aus diesem Grund ist darauf zu achten, dass die Kosten der zusätzlich benötigten Fahrzeughard- und -software (W1) und der Aufwand der Registrierung neuer VANET-Teilnehmer möglichst gering gehalten wird (W2). Es ist zu beachten, dass ggf. auch initiale Kosten für den Aufbau eines stationären Netzes und Unterhaltskosten für zentrale Instanzen anfallen können. Alle Aufgaben sind einerseits möglichst kostengünstig zu bewältigen (W3), andererseits soll der Betreiber der Infrastruktur die Akzeptanz aller VANET-Beteiligten genießen (W4). Ggf. sind die verschiedenen Aufgaben auf unterschiedliche Institutionen zu verteilen.

I1	Inhaltsintegrität
I2a	Eindeutige Senderauthentifizierung für A2
I2b	Nachträgliche Zurechenbarkeit für A1 und A3
V1	Verschiedene Vertraulichkeitsstufen
V2	Vertraulichkeit administrativer Nachrichten
V3	Schutz der Sicherheitsinfrastruktur
D1	Schutz vor Profilerstellung
D2	Schutz vor Überwachung
D3	Schutz der Sender- und Empfängeridentität
P1	Effizienz bei Rechenkapazität und Bandbreite
W1	Niedrige Kosten für Fahrzeughard- und Software
W2	Wenig Aufwand bei der Registrierung
W3	Betrieb möglichst kostengünstig
W4	Akzeptanz der Teilnehmer

Tabelle 1: Anforderungen

3 Grundsätzliche Überlegungen

Im Folgenden werden einige grundsätzliche Fragen angesprochen, die die konkrete Ausgestaltung der Sicherheitsinfrastruktur beeinflussen. Es wird diskutiert, was als Identität eines Teilnehmers herangezogen und wie die Authentifizierung der Teilnehmer erfolgen soll.

3.1 Identität

Eine Identität liefert die Grundlage für jegliche Authentifizierung, d.h. sie stellt ein gewisses Wiedererkennungsmerkmal dar, anhand dessen man z.B. korrekt funktionierende bzw. kooperative Teilnehmer zum VANET zulassen und fehlerhafte bzw. böswillige ausschließen kann. Das impliziert natürlich, dass ein Knoten weder anonym auftreten noch seine Identität beliebig ändern können darf, da sonst sämtliche Maßnahmen der Regulierung ins Leere greifen. Die Natur einer Identität in VANETs ist zunächst nicht eindeutig festgelegt. Eine VANET-Identität kann Identitätsmerkmale des Fahrzeugs, des aktuellen Fahrers oder Halters oder von beiden zusammen beinhalten.

Fahrzeugbezogene Identität

In VANETs treten neben eventuell personenbezogenen Daten in Masse fahrzeugbezogene, oft automatisch versendete Daten (z.B. Telematiknachrichten) auf. Zudem ist es durchaus möglich, dass der aktuelle Fahrer nicht für eventuelle Falschmeldungen verantwortlich ist, sondern diese von einem Defekt des Fahrzeugs oder von Manipulationen herrühren. Für diesen Fall erscheint eine fahrzeugbezogene Identität sehr geeignet.

Sollen gestohlene oder in Straftaten verwickelte Fahrzeuge verfolgt werden, müssen Identitätsmerkmale des Fahrzeugs (wie z.B. Fahrgestellnummer, Nummernschild usw.) als zwingend notwendiger Bestandteil einer VANET-Identität betrachtet werden. Dies entspricht in digitaler Form der gegenwärtigen Situation: Ein Nummernschild pseudonymisiert den Halter eines Fahrzeugs, der Fahrer kann nicht mit Sicherheit bestimmt werden. Eine solche fahrzeugbezogene Identität wäre direkt im Fahrzeug in manipulationssicherer Hardware zu speichern.

Personenbezogene Identität

Die zweite Variante sind personenbezogene VANET-Identitäten, die sich direkt auf den Fahrer des entsprechenden Fahrzeugs beziehen, da alle Nachrichten direkt mit dessen Fahrweise bzw. dem

Zustand seines Fahrzeugs zusammenhängen. Dieser Ansatz erleichtert auch die Rekonstruktion von Unfall- und Fahrerflucht-Situationen, bei denen bisher nur das Unfallfahrzeug und damit der Halter, nicht aber der Fahrer mit Sicherheit bestimmt werden konnte, wenn dieser sich dem Tatort entzogen hatte.

Dem steht jedoch die aktuelle Gesetzgebung gegenüber, die grundsätzlich den Fahrzeughalter (§7 StVG) haftbar macht[1]. Den Hinweis auf den Fahrzeughalter leisten ohne großen Aufwand auch rein fahrzeugbezogene Identitäten, da die Exekutive bereits heute die Halter über Dokumente wie Fahrzeugschein und -brief bzw. Zulassungsbescheinigung Teil 1 und Teil 2 oder über ihre zentralen Speicher ermittelt.

Allerdings erscheint es angebracht, zumindest für diejenigen Teilnehmer eines VANETs personenbezogene Identitäten zu verwenden, die über erhöhte Privilegien verfügen, wie z.B. Einsatzkräfte der Polizei, Feuerwehr, etc. Es stellt sich dann allerdings die Frage, wie entschieden werden kann, ob eine Person ihre Privilegien gerade benutzen darf. Ein Polizist sollte beispielsweise, wenn er außerhalb seiner Dienstzeit im Privat-KFZ unterwegs ist, keine Anweisungen an andere Verkehrsteilnehmer senden können. Dieses Problem adressieren die weiter unten diskutierten gemischten Identitäten.

Die Vielzahl möglicher Fahrer wirft auch die Frage auf, wo personenbezogene Identitäten gespeichert werden sollten. Eine Vorinstallation auf dem Fahrzeug selbst scheidet aus, da man nicht vorhersehen kann, welche Personen das Automobil benutzen werden. Als weitere Variante eignen sich auch die Fahrzeugschlüssel nicht: Zum einen kann aus Kostengründen nicht für jeden Fahrer ein eigener Schlüssel vorausgesetzt werden, zum anderen läge die Verwaltung und Speicherung des kryptographischen Materials ohne Ausweichmöglichkeit in den Händen der Automobilhersteller.

Elektronische Führerscheine hingegen bieten sich an: Jeder Fahrer muss sowieso einen gültigen Führerschein besitzen und ihn bei Bedarf nachweisen[2], d.h. mit sich führen. Das Speichern der Identität auf einem elektronischen Führerschein in Form einer Smartcard bedeutet also kaum einen Komfortverlust für die VANET-Benutzer, es müsste allerdings der bisherige Führerschein umgetauscht werden.

Bei dieser Lösung ergeben sich Synergieeffekte in Bezug auf die Neuregelung der Lenk- und Ruhezeiten (VO 3820/85), deren Umsetzung für Mai 2006 erwartet wird [Ind06]. In Folge dieser Neuregelung werden sog. Fahrerkarten an Führer von Kraftfahrzeugen ausgegeben, die unter VO 3820/85 fallen. Die Fahrerkarte ist „ein von den Behörden des Mitgliedstaates zugeteiltes entnehmbares, persönliches Übertragungs- und Speichermedium eines Fahrers für dessen Identifizierung und die Speicherung der wichtigsten Daten“ (Verordnung (EG) Nr. 2135/98, Anhang I B). Man könnte diese Fahrerkarte also ohne große Probleme als elektronischen Führerschein ausbauen und auch für die Identifizierung in VANETs benutzen.

Würde nun ein solcher elektronischer Führerschein vom Fahrzeug zwangsweise zum Starten vorausgesetzt, könnte sich ein Fahrzeughalter beim Verleihen seines Fahrzeugs an einen anderen Fahrer gegen Ansprüche aus nicht von ihm verursachten Situationen absichern. Außerdem könnte der Halter genau definieren, wer mit dem Fahrzeug fahren darf. Auch das Fahren ohne gültigen Führerschein könnte eingedämmt werden. Ein solcher Zwang ist bisher rechtlich aber nicht durchzusetzen und darüber hinaus aus folgenden Gründen auch nicht wünschenswert: Bei einem Identifizierungszwang durch das Fahrzeug könnten sich z.B. Probleme ergeben, wenn ein Fahrzeug in einem Notfall bewegt werden müsste, aber kein nachweislich berechtigter Fahrer vor Ort ist. Unter Umständen könnte es auch passieren, dass sich der Halter versehentlich die Rechte an seinem Fahrzeug entzieht und dann nicht mehr damit fahren kann. Abgesehen von diesen Problemen ist es

[1] Der Fahrzeugführer ist allerdings auch ersatzpflichtig (§18 StVG).
[2] Laut §2 Abs. 1 StVG ist die Fahrerlaubnis „durch eine amtliche Bescheinigung (Führerschein) nachzuweisen.“ Wer ihn während der Fahrt nicht mitführt, begeht eine Ordnungswidrigkeit nach §75 Nr. 4 FeV (vgl. [DDD04]).

zum Schutz der Privatsphäre nicht wünschenswert, dass man sich grundsätzlich vor Fahrtbeginn vor dem Fahrzeug ausweisen muss.

Gemischte Identität

Bei diesem Ansatz, der Nachrichten sowohl dem Fahrzeug als auch dem Fahrer zurechenbar macht, werden personen- und fahrzeugbezogene Identitätsmerkmale kombiniert. Sollen erhöhte Privilegien benutzt werden, müssen beide Identitäten das unterstützen. Anweisungen z.B. zum Räumen einer Fahrbahn wären somit nur gültig, wenn sie von einem berechtigten Fahrzeug (z.B. einem Krankenwagen) mit einem berechtigten Fahrer kommen. Dadurch kann verhindert werden, dass gestohlene Einsatzfahrzeuge zum Aussenden von Anweisungen über das VANET missbraucht werden.

Nachteil dieser Variante ist, dass für die Erstellung von Bewegungsprofilen per se die meisten Informationen bereitgestellt werden. Sind die Identitäten ungeschützt in den Nachrichten enthalten, kann ein Angreifer sowohl bestimmte Personen als auch bestimmte Fahrzeuge problemlos verfolgen. Das Problem der Bewegungsprofilerstellung ergibt sich aber auch bei den anderen Varianten, wenn die Identitäten ungeschützt verwendet werden. Unter ungeschützt ist dabei zu verstehen, dass die Identitäten einerseits im Klartext übertragen und andererseits auch nicht gewechselt werden.

Zudem entstehen möglicherweise Mehrkosten dadurch, dass zwei Identitäten benötigt werden. Es muss nämlich einerseits die fahrzeugbezogene Identität erzeugt und in manipulationssicherer Hardware im Fahrzeug gespeichert werden, als auch andererseits die personenbezogene Identität auf einem elektronischen Führerschein.

Fazit

Ausgehend von der momentan geltenden Rechtslage erscheint eine fahrzeugbezogene Identität angemessen mit deren Hilfe der Halter des Fahrzeugs ermittelt werden kann. Für spezielle Personengruppen wie Polizisten sollten allerdings zusätzlich personenbezogene Identitäten verwendet werden, an die ihre speziellen Privilegien gebunden sind. Die Privilegien gelten dann nur im Zusammenspiel von fahrzeugbezogener und personenbezogener Identität.

Für bestimmte Situationen, wie z.B. für den gewerblichen Verleih von Fahrzeugen, erscheint es sinnvoll zusätzlich zur fahrzeugbezogenen auch eine personenbezogene Identität für „normale“ Fahrer zu benutzen, um den Halter in gewissem Maße vor Ansprüchen Dritter zu schützen. In diesem Fall ist allerdings eine nachträgliche Identifizierung des Fahrers ausreichend. Die personenbezogene Identität muss hier also nicht zwangsläufig im VANET verwendet werden, sondern könnte zusammen mit der Fahrzeit und ggf. anderen Daten in manipulationssicherer Hardware im Fahrzeug gespeichert werden. Diese Daten sind dann allerdings vor unbefugtem Auslesen zu schützen. Ein elektronischer Führerschein zur Zugangskontrolle zum Fahrzeug erscheint als Option durchaus sinnvoll, sollte allerdings keinesfalls zwangsweise zur VANET-Identität gehören.

3.2 Authentifizierung

In diesem Abschnitt soll geklärt werden, wie die Authentifizierung im VANET erfolgen soll. Grundsätzlich kommt dafür symmetrische oder asymmetrische Kryptographie in Frage. Die Vorverteilung des benötigten kryptographischen Materials ist hier kein so großes Problem, wie in anderen Ad-hoc-Netzen, da sich im Lebenszyklus eines Fahrzeugs mindestens die Zeitpunkte „Herstellung“ und „Zulassung/Umschreibung bei der Zulassungsbehörde“ dafür eignen. Im Zuge der periodischen Inspektionen eines Fahrzeugs kann auch geprüft werden, ob die Schlüsselspeicher in der Zwischenzeit manipuliert wurden [PP05].

Symmetrische Kryptographie

Bei symmetrischer Kryptographie müssen zwei Kommunikationspartner A und B denselben Schlüssel verwenden, d.h. beide kennen den Authentifizierungsschlüssel. Dies wird zum Problem, wenn die Authentifizierung nicht gegenüber einer vertrauenswürdigen Stelle (Trusted Third Party, TTP) erfolgt. Dann nämlich kennt der (nicht vertrauenswürdige) Kommunikationspartner B den Authentifizierungsschlüssel von A und kann sich in Folge als A ausgeben. Man verliert ohne weiterführende Maßnahmen die Zurechenbarkeit bzw. Nichtabstreitbarkeit der Nachrichten. Abgesehen davon wäre es sowieso nicht möglich, in allen Fahrzeugen die Schlüssel aller anderen Fahrzeuge zu speichern.

Möglich wäre symmetrische Kryptographie zur Authentifizierung in Verbindung mit einer TTP, die dann die Autorisierung zur Teilnahme am VANET bestätigt (z.B. durch spezielle Schlüssel oder Zertifikate). Nachteil dieser Variante ist, dass man am VANET erst teilnehmen kann, nachdem man sich bei der TTP authentifiziert hat. Die zuverlässige Erreichbarkeit einer solchen TTP kann in einem Ad-hoc-Netz aber nicht vorausgesetzt werden, d.h. eine Teilnahme am VANET sollte (zumindest eingeschränkt auf verkehrssicherheitskritische Nachrichten) auch möglich sein, ohne sich bei einer zentralen TTP authentifizieren zu müssen.

Asymmetrische Kryptographie

Genau diese Möglichkeit bietet Authentifizierung auf Basis von asymmetrischer Kryptographie. Hier besitzt jeder Teilnehmer seinen eigenen privaten Schlüssel und den dazugehörigen öffentlichen Schlüssel, der mit Hilfe einer Public Key Infrastruktur (PKI) in einem Zertifikat einer Identität zugeordnet wird. Ein Kommunikationspartner kann mit Hilfe des Zertifikats und dem darin enthaltenen öffentlichen Schlüssel die Authentifizierung (Signatur) einer Nachricht prüfen, selbst aber keine (gefälschte) Authentifizierung vornehmen.

Die Zertifikate der Kommunikationspartner können mit den Nachrichten übermittelt werden, es ist ausreichend das jeweils eigene Schlüsselpaar samt Zertifikat und die Wurzelzertifikate der PKI in den Fahrzeugen zu speichern. Ein weiterer Vorteil besteht darin, dass der private Schlüssel das Fahrzeug nicht zwangsweise verlassen muss. Er kann in sicherer Hardware im Fahrzeug (bzw. ggf. auch im elektronischen Führerschein) erzeugt und gespeichert werden.

Der wohl schwerwiegendste Nachteil asymmetrischer Kryptographie sind die im Vergleich zu symmetrischer Kryptographie sehr langen Zeiten, die zur Signaturgenerierung bzw. -verifizierung benötigt werden. Ein weiterer Nachteil ist, dass Informationen zu Zertifikatsrückrufen verteilt werden müssen.

Fazit

Zur Basis-Authentifizierung sollte asymmetrische Kryptographie in Verbindung mit einer PKI eingesetzt werden, da dies dem Ad-hoc-Charakter von VANETs am besten entspricht. Jeder Besitzer eines gültigen Zertifikats kann authentifizierte Nachrichten im VANET versenden und andere Teilnehmer beispielsweise auf Gefahrensituationen aufmerksam machen. Wenn möglich sollte nach einer Basis-Authentifizierung allerdings aufgrund des Performancevorteils symmetrische Kryptographie für die Verschlüsselung und Nachrichten-Authentifizierung nicht verkehrssicherheitskritischer Nachrichten verwendet werden.

4 Vorschlag für eine Sicherheitsinfrastruktur

Im Folgenden wird basierend auf den Erkenntnissen der vorhergehenden Kapitel ein Vorschlag für eine VANET-Sicherheitsinfrastruktur präsentiert, die möglichst sicher und effizient gestaltet ist. Sie sieht die Verwendung asymmetrischer Kryptographie für verkehrssicherheitskritische Nachrichten vor, die nach erstmaliger Initialisierung fast gänzlich ohne zentrale Stellen bzw. den Kontakt zu zentralen Einrichtungen auskommt. Alle anderen Nachrichten werden durch ein System mit

symmetrischer Kryptographie abgesichert, das wesentlich performanter ist und die Privatsphäre der Teilnehmer besser schützt. Nach der Beschreibung der einmaligen Initialisierung (4.1) folgt eine genauere Erläuterung des alltäglichen Betriebs (4.2) mit den asymmetrischen und symmetrischen Verfahren.

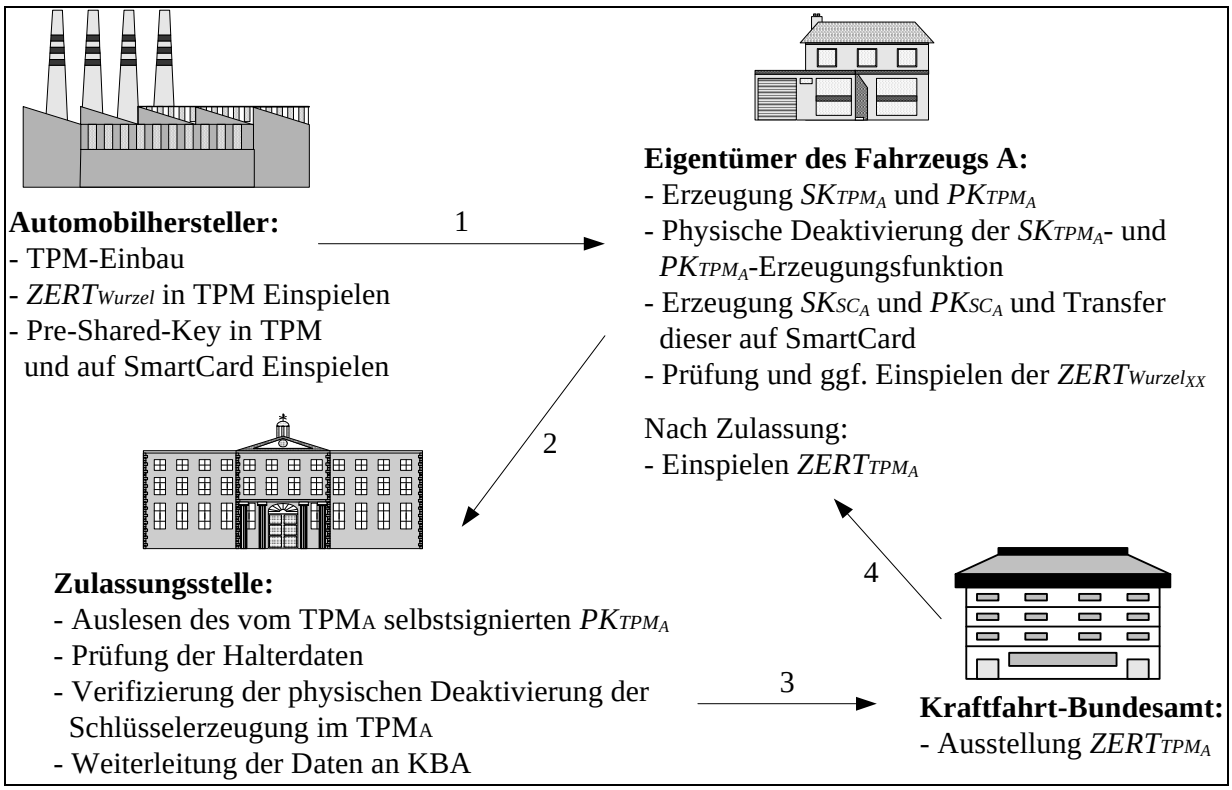

Abbildung 1: Initialisierung

4.1 Initialisierung

Jedes Fahrzeug besitzt manipulationssichere Hardware (ein sog. Tamper Proof Module, TPM), die beim Herstellungsprozess fest mit dem Fahrzeug verbunden wird. In diesem TPM wird vom Automobilhersteller das Wurzelzertifikat ($ZERT_{Wurzel}$) des Landes installiert, in das das Fahrzeug verkauft wird, z.B. $ZERT_{Wurzel_{DE}}$ für Deutschland. Zusätzlich wird ein symmetrischer Schlüssel aufgespielt, der auch auf einer SmartCard enthalten ist, die der Käufer erhält und auf der bei der Initialisierung des TPM durch den Käufer weitere Authentifizierungsschlüssel gespeichert werden (siehe Abbildung 1). Dieser symmetrische Pre-Shared-Key dient zur Verschlüsselung der Kommunikation zwischen TPM und SmartCard (Anforderung V2 und V3).

Nachdem der Käufer sein Fahrzeug (und die SmartCard) erhalten hat, verbindet er das TPM mit der SmartCard und startet den Initialisierungsprozess. Das TPM prüft daraufhin zuerst die Verbindung mit der SmartCard und erstellt dann zwei Schlüsselpaare. Eines davon dient als Schlüsselpaar des TPM (z.B. PK_{TPM_A} und SK_{TPM_A} für Fahrzeug A) und wird dort gespeichert, wobei das TPM dafür sorgt, dass maximal ein Schlüsselpaar im TPM gespeichert ist. Der zugehörige private Schlüssel (SK_{TPM_A}) verlässt das TPM nicht (Anforderung V3). Das zweite Paar wird dann mit Hilfe des ersten signiert und auf der SmartCard gespeichert. Optional kann der Zugriff auf den privaten Schlüssel (SK_{SC_A}) auf der SmartCard mit einem Passwort geschützt werden, das beim Initialisierungsprozess abgefragt wird.

Das signierte Schlüsselpaar (PK_{SC_A} und SK_{SC_A}) auf der SmartCard dient zur Authentifizierung des Käufers. Konfigurationsänderungen wie z.B. das Einspielen oder Löschen von Wurzelzertifikaten am TPM können nur nach erfolgreicher Authentifizierung mit diesem Schlüsselpaar vorgenommen werden. Dadurch wird sichergestellt, dass ausschließlich der Käufer zu solchen Konfigurationsänderungen berechtigt ist. Wird das Fahrzeug verkauft, kann der neue Eigentümer

die alten Authentifizierungsschlüssel im TPM löschen und sich neue erzeugen. Sind keine Fehler aufgetreten, muss der Käufer nun die Möglichkeit zur Erzeugung eines TPM-eigenen Schlüsselpaars (PK_{TPM_A} und SK_{TPM_A}) physisch (z.B. durch das Vernichten einer dafür vorgesehenen Sicherung mit Überspannung) deaktivieren, wodurch sichergestellt wird, dass die Identität des Fahrzeugs, die dem öffentlichen Schlüssel PK_{TPM_A} entspricht, nicht mehr gewechselt werden kann (zumindest solange das TPM nicht ausgetauscht wird).

Von der Zulassungsstelle als Registration Authority[3] wird bei der erstmaligen Zulassung und bei Umschreibungen des Fahrzeugs der selbstsignierte öffentliche Schlüssel des TPM ausgelesen und überprüft, ob die Funktionen zur Erzeugung eines TPM-eigenen Schlüsselpaars deaktiviert sind. Danach werden die üblichen Dokumente zur Identifizierung des Fahrzeughalters überprüft und zusammen mit dem selbstsignierten öffentlichen Schlüssel des TPM an das Kraftfahrt-Bundesamt (KBA) als Certification Authority geschickt. Dieses erstellt damit ein Zertifikat für das Fahrzeug ($ZERT_{TPM_A}$), das der Halter in das TPM einspielt. Das TPM kann anhand des vorhandenen $ZERT_{Wurzel_{DE}}$ überprüfen, ob das Zertifikat von einer vertrauenswürdigen Instanz korrekt ausgestellt wurde. Es handelt sich bei der VANET-Identität also um eine fahrzeugbezogene Identität, die wie schon bisher mit den Daten des Halters verknüpft wird. Die Einrichtungen (Zulassungsstellen in den Landratsämtern und KBA) und Abläufe dazu sind prinzipiell schon vorhanden und werden von den Bürgern akzeptiert (Anforderung W4). Die Abläufe müssen nur noch um die neuen Schritte erweitert werden, was ohne großen Kostenaufwand[4] möglich ist (Anforderung W2 und W3). Die Absicherung der (drahtgebundenen) Kommunikation zwischen den Zulassungsstellen und dem KBA erfolgt ebenso wie die Absicherung der jeweiligen LANs und Rechner mit den bekannten Mitteln der Rechner- und Netzwerksicherheit, wie Firewalls, VPNs usw. und soll hier nicht näher erläutert werden.

Dadurch dass der Eigentümer überprüfen und bestimmen kann, welche Wurzelzertifikate im TPM installiert sind, wird verhindert, dass Fahrzeughersteller oder Werkstattpersonal unbemerkt eigene Zertifikatshierarchien aufbauen können, indem sie Wurzelzertifikate in die TPMs einschleusen. Andererseits ist natürlich dann auch der Eigentümer dafür verantwortlich zu machen, dass die nötigen Wurzelzertifikate z.B. beim Überschreiten von Landesgrenzen vorhanden sind.

4.2 Alltäglicher Einsatz

Fahrzeug A kann nun mit $ZERT_{TPM_A}$ am VANET teilnehmen und digital signierte Nachrichten versenden. Wird $ZERT_{TPM_A}$ dabei jeder Nachricht angefügt, können die Empfänger die Integrität und mit Hilfe ihrer Wurzelzertifikate auch die Authentizität der Nachricht prüfen (Anforderungen I1 und I2a bzw. I2b). Abbildung 2 zeigt eine so gesicherte Nachricht.

Alle Nachrichten mit $ZERT_{TPM_A}$ zu signieren und dieses mitsamt der Nachricht zu versenden, ist allerdings weder aus Performance- (Anforderung P1) noch aus Privacy-Aspekten (Anforderungen D1, D2 und D3) zu begrüßen. Aus diesem Grund werden lokal verteilte unabhängige TTPs vorgeschlagen, die Nachrichtenverschlüsselung und -authentifizierung innerhalb ihrer zugewiesenen geographischen Gebiete mit symmetrischer Kryptographie ermöglichen.

Bevor die Funktionsweise der TTPs genauer erläutert wird, soll geklärt werden, wann symmetrische und wann asymmetrische Kryptographie zum Einsatz kommen soll. Asymmetrische Kryptographie kann wie oben angedeutet sofort nach dem Initialisierungsprozess verwendet werden. Symmetrische Kryptographie setzt (wie im Folgenden noch genauer erläutert wird) den (zumindest einmaligen) Kontakt zu einer der TTPs voraus. Konnte ein VANET-Teilnehmer seine zuständige TTP noch nicht kontaktieren, muss er asymmetrische Kryptographie verwenden und kann

[3] Die Zulassungsstellen und das Kraftfahrt-Bundesamt werden hier beispielhaft für die entsprechenden Institutionen anderer Länder genannt.

[4] Hier sei auch darauf hingewiesen, dass das KBA seit 2005 ein Trustcenter für das Zentrale Kontrollgerätekartenregister (ZKR) betreibt und somit im Prinzip schon eine Certification Authority ist (siehe [KB06]).

Nachrichten, die mit symmetrischer Kryptographie gesichert sind, weder verstehen noch verifizieren.

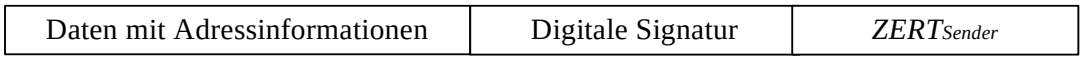

Abbildung 2: Asymmetrisch gesicherte Nachricht

Verkehrssicherheitskritische Nachrichten, wie Stau- oder Unfallwarnungen sowie Alarmsignale und Anweisungen, müssen daher mit asymmetrischer Kryptographie gesichert, d.h. mit einer digitalen Signatur versehen werden. Diese Nachrichten müssen, wie auch schon in Kapitel 2.2 erläutert, nicht verschlüsselt werden, da normalerweise keine nicht öffentlichen Informationen enthalten sind. Lediglich im Fall einer von einer Privatperson versandten Warnung wird – unter Umständen unerwünscht – die Information preisgegeben, dass diese Person zu einem bestimmten Zeitpunkt an einem bestimmten Ort ist bzw. war. Da Warnungen aber eher selten und nur für ein relativ begrenztes geographisches Gebiet erzeugt werden, können diese Informationen nicht bzw. nur sehr schwer zur Bewegungsprofilerstellung verwendet werden. Aus diesem Grund erscheint es hier angebracht die Verkehrssicherheit über das durchaus berechtigte Interesse des Einzelnen unerkannt zu bleiben zu stellen. Alle anderen Nachrichten werden mit dem symmetrischen Verfahren gesichert. Ein VANET-Teilnehmer, der den Initialisierungsprozess abgeschlossen hat, kann somit sowohl alle kritischen Nachrichten, die die Verkehrssicherheit betreffen, empfangen und verifizieren, als auch selbst Warnungen bei besonders kritischen Situationen versenden. Die weniger kritischen Nachrichten, wie die periodisch gesendeten Telematiknachrichten oder die Nachrichten der Komfort-Dienste, können erst nach Kontakt mit der TTP bearbeitet werden. Dies bietet auch die Möglichkeit, Störer aus dem VANET auszuschließen, ohne ihnen die verkehrssicherheitskritischen Nachrichten vorzuenthalten.

Um solche Störer auch davon abzuhalten, Warnungen zu versenden, könnten Rückruflisten verteilt werden, die periodisch im TPM eingespielt werden müssen. Dies kann durch den Eigentümer selbst erfolgen oder er kann seine Werkstatt dazu autorisieren. Diese könnte dazu ein vom TPM des Fahrzeugs selbstsigniertes Schlüsselpaar erhalten, in dem vermerkt ist, dass nur Rückruflisten eingespielt werden dürfen. Da Warnungen eines anderen VANET-Teilnehmers nicht zwangsläufig befolgt werden müssen, sind diese Rückruflisten allerdings nicht als kritisch einzustufen. Der Fahrer kann seine fahrzeuginternen Sensoren und die Nachrichten anderer VANET-Teilnehmer zur Plausibilitätsprüfung beim Empfang einer Warnung verwenden. Erhält er beispielsweise eine Warnung, dass wenige Kilometer vor ihm ein Stau beginnt, aber keine einzige Telematikinformation eines anderen VANET-Teilnehmers, die auf stehenden oder langsamen Verkehr hindeutet, so kann er mit hoher Wahrscheinlichkeit davon ausgehen, dass es sich um eine gefälschte Warnmeldung handelt, da in einem Stau viele Fahrzeuge ebensolche Telematikinformationen senden müssten.

Bei den Alarmmeldungen und Anweisungen ist die Sachlage anders. Diese sind unverzüglich zu befolgen. Hier bietet die digitale Signatur den Vorteil, dass genau nachvollzogen werden kann, von wem die Nachricht stammt und ob dieser berechtigt ist, eine solche Nachricht zu senden (Anforderung I1 und I2a). Um dem Empfänger zu erlauben, diese Berechtigung zu prüfen, können entweder entsprechende Attribute in das Zertifikat aufgenommen oder gesonderte Attributzertifikate verwendet werden. Die Attributzertifikate haben den Vorteil, dass sie für sehr kurze Zeiträume, z.B. für einige Minuten oder Stunden, erstellt werden können. Der Empfänger muss also nicht unbedingt eine Zertifikatsrückrufliste prüfen, bevor er die Nachricht akzeptiert. Auch kann die Autorisierung für das angeforderte Privileg vor Ausstellung des Attributzertifikats besser geprüft werden. So wird z.B. das Attributzertifikat, das das Aussenden von Anhalteanweisungen der Polizei erlaubt, von der zuständigen Stelle erst ausgestellt, nachdem sich das Fahrzeug als Polizeifahrzeug und der Fahrer z.B. mit Hilfe seines elektronischen Führerscheins als Polizist authentifiziert haben. Gestohlene Einsatzfahrzeuge können somit nicht mehr zum

Versenden von Anweisungen im VANET missbraucht werden. Auch der ungerechtfertigte Einsatz von Privilegien kann einer bestimmten Person eindeutig zugewiesen werden.

Absicherung mit symmetrischer Kryptographie

Um am symmetrisch gesicherten Teil des VANETs teilnehmen zu können, verbindet sich der VANET-Teilnehmer A über das VANET oder ein anderes Netz, wie etwa GSM, mit seiner lokalen TTP und authentifiziert sich über ein Challenge-Response-Verfahren mit $ZERT_{TPM_A}$. Nachdem sich auch die TTP authentifiziert hat, erhält er von ihr ein Pseudonym *PA* unter dem er dann im VANET auftritt sowie drei symmetrische Schlüssel k_C, $k_{MAC_{ALL}}$, $k_{MAC_{PA}}$ (siehe Abbildung 3) deren Funktion im Folgenden noch genauer erläutert wird. Die Kommunikation zwischen A und der TTP ist dabei natürlich zu verschlüsseln (Anforderung V2 und V3). Die dazu notwendigen Schlüssel können beispielsweise mit einem Diffie-Hellman-Schlüsselaustausch erzeugt werden. Von der Verwendung der Zertifikate $ZERT_{TPM_A}$ und $ZERT_{TTP}$ zur Verschlüsselung sollte abgesehen werden, da diese der Authentifizierung dienen. Die TTPs müssen natürlich, ebenso wie die Zulassungsstellen und das KBA, mit den üblichen Mechanismen der Rechner- und Netzwerksicherheit vor unbefugtem Zugriff geschützt werden (Anforderung V3).

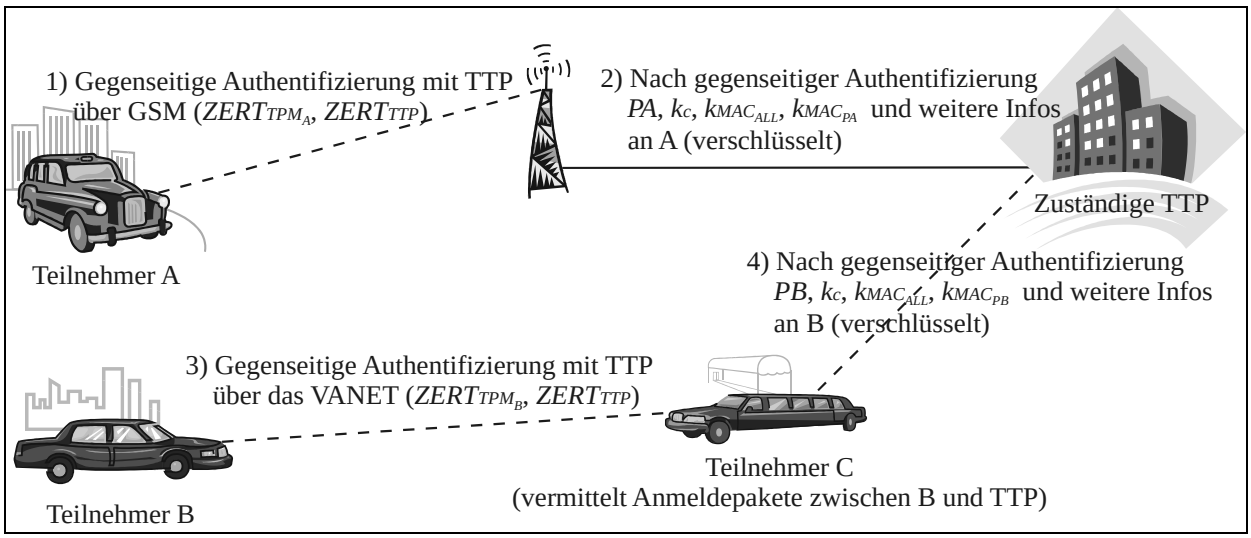

Abbildung 3: Anmeldung von Teilnehmer A (Schritt 1 und 2) und B (Schritt 3 und 4) im symmetrisch gesicherten VANET-Teil

Für alle VANET-Teilnehmer im Gebiet der TTP ist k_C und $k_{MAC_{ALL}}$ gleich. Sie benutzen nun k_C, um ihre Nachrichten symmetrisch zu verschlüsseln. Außenstehende, die nicht am VANET teilnehmen und k_C nicht kennen, erhalten keine Informationen über die ausgetauschten Nachrichten (Anforderung V1). Geht man so weit, auch die Adressinformationen zu verschlüsseln, erhalten Außenstehende aufgrund des Broadcast-Charakters der drahtlosen Datenübertragung nicht einmal mehr Informationen darüber, wer mit wem kommuniziert (Anforderung D3). Bei den Empfängern entsteht dadurch allerdings ein etwas erhöhter Aufwand, da zumindest der Anfang jeder Nachricht entschlüsselt werden muss, um herauszufinden, an wen die Nachricht adressiert ist. Für die Komfort-Dienste können über die Basis-Verschlüsselung mit k_C hinaus natürlich auch eigene anwendungsspezifische Schlüssel und Zertifikate zur vertraulichen Ende-zu-Ende-Kommunikation eingesetzt werden (Anforderung V1).

Vor der Verschlüsselung wird jeder Nachricht *PA* hinzugefügt, um den Absender zu kennzeichnen, und dann ein Hashed Message Authentication Code (HMAC) über die Nachricht gebildet, in den $k_{MAC_{PA}}$ eingeht. Anhand dieses HMAC kann TTP im Nachhinein prüfen, ob die Nachricht wirklich von PA stammt (Anforderung I2b). Da die Kommunikationspartner von PA dessen $k_{MAC_{PA}}$ nicht kennen (dürfen), können sie diesen HMAC nicht zur Integritätsprüfung verwenden. Aus diesem Grund wird über die gesamte Nachricht (inklusive des ersten HMAC) ein weiterer HMAC gebildet, in den $k_{MAC_{ALL}}$ eingeht. Diesen kennen nun wieder alle VANET-Teilnehmer im Gebiet der TTP und

können somit die Integrität der Nachricht verifizieren (Anforderung I1). Abbildung 4 zeigt den Aufbau einer so gesicherten Nachricht. Damit dieses System funktioniert und keine Nachrichten von VANET-Teilnehmern gefälscht werden können, dürfen die drei symmetrischen Schlüssel nur im TPM im Klartext vorhanden sein. Alle Ver- und Entschlüsselungsvorgänge sowie das Erstellen, Anfügen und Prüfen der HMACs müssen also im TPM erfolgen (Anforderung V3). Auch der Fahrzeugeigentümer darf keinen Zugriff auf die symmetrischen Schlüssel erhalten oder die Nachrichtenerstellung beeinflussen können.

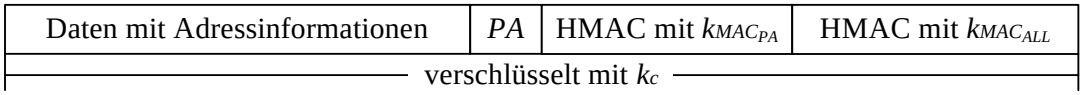

Abbildung 4: Symmetrisch gesicherte Nachricht

Die Schlüssel k_C und $k_{MAC_{ALL}}$ werden periodisch gewechselt. Den Zeitpunkt der Wechsel bekommen die VANET-Teilnehmer von der TTP mitgeteilt und müssen sich die neuen Schlüssel besorgen, indem sie sich wieder mit der TTP in Verbindung setzen. Die Wechselintervalle sollten dabei weder zu lang (Knacken der Schlüssel wäre möglich) noch zu kurz (TTP muss zu oft kontaktiert werden) sein. Ein sinnvoller Vorschlag scheint ein täglicher Wechsel der Schlüssel um ca. 3:00 Uhr nachts zu sein. Zu diesem Zeitpunkt sind nicht viele Fahrzeuge unterwegs und die TTP erlebt keine Lastspitze, da sich jeder VANET-Teilnehmer dann nur einmal täglich beim Antritt der ersten Fahrt mit der TTP verbinden muss. Ggf. könnte die TTP auch schon einige Stunden vor dem Wechsel damit beginnen, den VANET-Teilnehmern die neuen Schlüssel mitzuteilen.

Das Pseudonym *PA* und der zugehörige Schlüssel $k_{MAC_{PA}}$ können auf Anforderung des VANET-Teilnehmers oder nach Ablauf einer bestimmten Zeitspanne gewechselt werden. Es ist auch vorstellbar, dass ein Teilnehmer gleich mehrere Pseudonyme zugeteilt bekommt, die er dann nach eigenem Ermessen einsetzen und wechseln kann (Anforderung D1 und D3). Die TTP speichert die Zuordnungen von Pseudonymen zu Identitäten, die sie anhand der Authentifizierungszertifikate feststellen kann (Anforderung I2b). Die TTP ist dazu verpflichtet, die anfallenden Daten vor unberechtigtem Zugriff zu schützen. Stört allerdings ein VANET-Teilnehmer die korrekte Funktion des VANETs (z.B. durch Einspeisen falscher Meldungen) kann die TTP nach Prüfung der Sachlage die Identität des Teilnehmers aufdecken und diesen ggf. auch von der weiteren Teilnahme am VANET ausschließen, indem sie ihm keine neuen Pseudonyme und Schlüssel zuteilt. Das genaue Vorgehen zur Prüfung der Sachlage und wann die Identität eines Teilnehmers aufgedeckt werden soll, würde hier zu weit führen, müsste allerdings genau spezifiziert werden, um z.B. eine automatische Überwachung oder Strafverfolgung bei kleineren Verstößen gegen die StVO auszuschließen (Anforderung D2). Aus diesem Grund erscheinen unabhängige Datenschutzorganisationen (oder auch Einrichtungen wie das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD)) als Betreiber der lokalen TTPs am geeignetsten (Anforderung W4). Es sei hier darauf hingewiesen, dass die lokalen TTPs sie Identität des Halters nicht kennen, da ihnen nur die fahrzeugbezogene Identität bekannt ist. Nur das KBA kann diese mit den Daten des Halters verknüpfen.

Eine Bewegungsprofilerstellung wird durch die ständig wechselnden Pseudonyme auch für Insider, die am VANET selbst teilnehmen, erschwert. Abhängig davon, wie die Pseudonyme von der TTP vergeben werden, kann dasselbe Pseudonym zu verschiedenen Zeitpunkten verschiedenen Teilnehmern zugeordnet sein. Es existiert also keine feste Zuordnung von Pseudonymen zu Identitäten.

Ein weiterer Vorteil der TTPs ist, dass sie über drahtgebundene Netze mit den Zulassungsbehörden in Kontakt stehen und dadurch immer über aktuelle Zertifikatsrückruflisten verfügen können. Wird das Zertifikat eines Teilnehmers zurückgerufen, werden die TTPs ihm keine neuen Pseudonyme und Schlüssel mehr mitteilen und ihm so den vollen Zugang zum Netz verwehren. Werden die

Schlüssel wie vorgeschlagen täglich gewechselt, kann er maximal 24 Stunden unberechtigt teilnehmen.

Bei der geographischen Verteilung der TTPs muss darauf geachtet werden, dass das zugeteilte Gebiet weder zu groß noch zu klein ist. Ist das Gebiet zu groß, ist die TTP für sehr viele Anfragen zuständig und es ist für die VANET-Teilnehmer unter Umständen schwierig über das Ad-hoc-Netz eine Verbindung zur TTP herzustellen. Ist das Gebiet zu klein, müssen die Schlüssel zu oft gewechselt werden. Den häufigen Schlüsselaustausch könnte man allerdings vermeiden, indem benachbarte TTPs dieselben k_C und $k_{MAC_{ALL}}$ verwenden. Hier soll auch darauf hingewiesen werden, dass die TTP dem Teilnehmer mitteilen muss, für welchen Bereich sie zuständig ist und wo er für die Verschlüsselung seiner Nachrichten andere Schlüssel verwenden muss. In den Grenzgebieten zwischen zwei TTPs könnten die Nachrichten ggf. auch doppelt versendet werden, um von Teilnehmern aus beiden Bereichen entschlüsselt und akzeptiert werden zu können. Bei der Aufteilung der Gebiete sollte man sich auch an typischen „Fahrmustern“ orientieren und beispielsweise die Grenzen in Kreisen um große Städte legen, da viele Bewohner ländlicher Gegenden typischerweise als Pendler in die nächstgelegene Stadt zur Arbeitsstelle fahren. Wie auch schon für die Wechselintervalle der Schlüssel sind hier aber noch genauere Untersuchungen erforderlich.

5 Fazit und Ausblick

Bisherige Ansätze für eine VANET-Sicherheitsinfrastruktur verwendeten entweder eine PKI (z.B. [RH05], [SE04], [Kar03]) oder setzten ausschließlich auf symmetrische Kryptographie (z.B. [PM04], [MBG06]). Die hier vorgeschlagene Kombination asymmetrischer und symmetrischer Kryptographie ermöglicht es, den in Kapitel 2 genannten Anforderungen an eine Sicherheitsinfrastruktur für VANETs wesentlich besser gerecht zu werden und die Vorteile beider Varianten auszunutzen, ohne gravierende Nachteile in Kauf nehmen zu müssen.

So ermöglicht es die vorgeschlagene Sicherheitsinfrastruktur die Integrität und Authentizität aller Nachrichten im VANET zu sichern, ohne dabei gravierende Performance-Einbußen oder Verletzungen der Privatsphäre hinnehmen zu müssen. Um beispielsweise Teilnehmer nur aus dem nicht verkehrssicherheitskritischen Teil des VANETs auszuschließen, müssen an die VANET-Teilnehmer nicht einmal Zertifikatsrückruflisten verteilt werden. Diese werden nur für den Total-Ausschluss eines Teilnehmers benötigt. Über Attribut-Zertifikate ist es möglich, gezielt erhöhte Privilegien zu vergeben, die vom Empfänger einer Nachricht aufgrund der kurzen Gültigkeitsdauer der Attribut-Zertifikate nicht erst mit Rückruflisten verifiziert werden müssen.

Es wurden im Gegensatz zu anderen Publikationen auch konkrete Vorschläge gemacht, wie die anfallenden Aufgaben verteilt werden sollten, um möglichst kostengünstig durchgeführt werden zu können. Mit dem Vorschlag, die Rolle der lokalen TTP auf unabhängige Datenschutzorganisationen zu übertragen, wird dem Interesse der VANET-Teilnehmer am Schutz ihrer Privatsphäre Rechnung getragen und verhindert, dass die anfallenden Daten von staatlicher Seite her missbraucht werden.

Der Vorschlag setzt zwingend manipulationssichere Hardware im Fahrzeug voraus, was durchaus als Nachteil angesehen werden kann. Eine solche manipulationssichere Hardware wird allerdings auch bei anderen Vorschlägen benötigt, da die verwendeten Schlüssel immer vor dem Zugriff möglichst aller Beteiligten zu schützen sind.

Wie in Kapitel 4.2 schon angedeutet sind noch genauere Untersuchungen in Bezug auf den Zeitraum der Schlüsselgültigkeit und der geographischen Verteilung der TTPs geplant. Auch das Prozedere zur Herausgabe der bei den TTPs gespeicherten Zuordnungen zwischen Identität und Pseudonym wird noch genauer spezifiziert werden.

Literaturverzeichnis

[DDD04] DR. JAGOW, Joachim ; DR. BURMANN, Michael ; DR. HEß, Rainer: *Straßenverkehrsrecht*. 18. Verlag C.H.Beck, 2004

[Eur03] EUROPEAN COMMISSION. *The Galilei Project - GALILEO Design Consolidation*. 2003

[Ind06] INDUSTRIE- UND HANDELSKAMMER FRANKFURT (ODER). *Merkblatt „Der digitale Tachograph“*. 2006

[Kar03] KARGL, Frank: *Sicherheit in Mobilen Ad hoc Netzwerken*. Ulm, Universität Ulm, Diss., 2003

[KB06] KRAFTFAHRT-BUNDESAMT. *Jahresbericht 2005: Digitales EG-Kontrollgerät im KBA*. 2006

[MBG06] MOUSTAFA, Hasnaa ; BOURDON, Gilles ; GOURHANT, Yvon: Providing Authentication and Access Control in Vehicular Network Environments. In: *Proceedings of IFIP SEC2006*, 2006

[MS02] MUNOZ, Jacob ; SYRACUSE, Natalia ; Internet Engineering Task Force (Hrsg.). *Proceedings of the 53. Internet Engineering Task Force*. 2002

[PM04] PIRZADA, Asad A. ; MCDONALD, Chris: Kerberos assisted Authentication in Mobile Ad-hoc Networks. In: *CRPIT ’04: Proceedings of the 27th conference on Australasian computer science*, 2004

[PNM06] PLÖßL, Klaus ; NOWEY, Thomas ; MLETZKO, Christian: Towards a Security Architecture for Vehicular Ad Hoc Networks. In: *Proceedings of ARES 2006*, 2006

[PP05] PARNO, Bryan ; PERRIG, Adrian: Challenges in Securing Vehicular Networks. In: *Proceedings of the Fourth Workshop on Hot Topics in Networks (HotNets-IV)*, 2005

[RH05] RAYA, M. ; HUBAUX, J. P.: The Security of Vehicular Ad Hoc Networks. In: *Proceedings of SASN‘05*, 2005

[SE04] SCHWINGENSCHLÖGL, Christian ; EICHLER, Stephan: Certificate-based Key Management for Secure Communications in Ad Hoc Networks. In: *Proceedings of the 5th European Wireless Conference: Mobile and Wireless Systems beyond 3G*, 2004

[TC03] TIAN, Jing ; COLETTI, Luca: Routing approach in CarTALK 2000 project. In: *Proceedings of the IST Mobile & Wireless Communications Summit 2003* Bd. 2, 2003