(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 1 975 900 A2**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
01.10.2008 Patentblatt 2008/40

(51) Int Cl.:
G08G 1/09 *(2006.01)*

(21) Anmeldenummer: **08102714.6**

(22) Anmeldetag: **18.03.2008**

(84) Benannte Vertragsstaaten:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT RO SE SI SK TR
Benannte Erstreckungsstaaten:
AL BA MK RS

(30) Priorität: **27.03.2007 DE 102007014649**

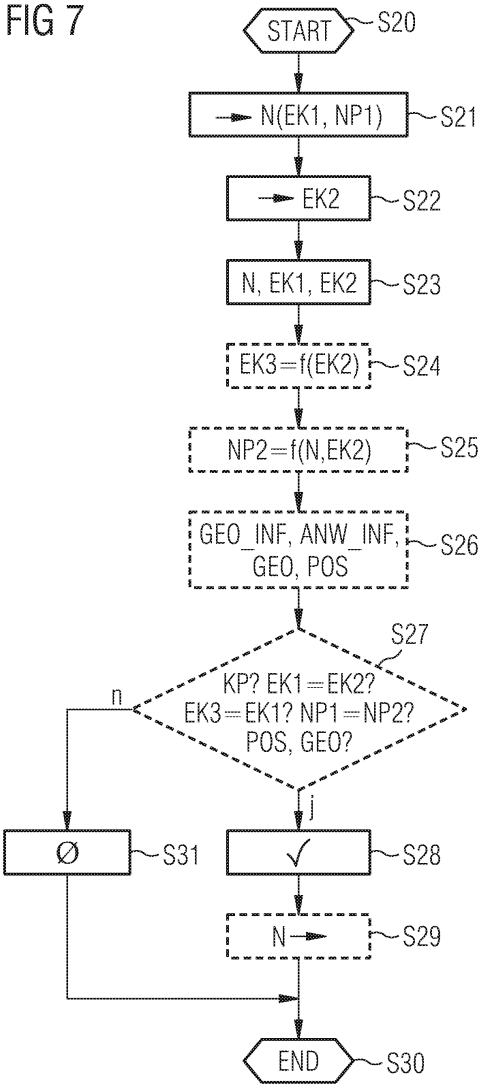
(71) Anmelder: **Continental Automotive GmbH**
30165 Hannover (DE)

(72) Erfinder:
- **Falk, Rainer**
  85386 Eching (DE)
- **Kohlmayer, Florian**
  82319 Starnberg (DE)

(54) **Verfahren und Vorrichtung zum Aussenden und Überprüfen von Nachrichten, die eine Einmalkennung oder einen Nachrichtenprüfwert umfassen**

(57) Eine Nachricht (N) umfasst eine erste Einmalkennung (EK1) oder einen abhängig von der ersten Einmalkennung (EK1) ermittelten ersten Nachrichtenprüfwert (NP1). Die Nachricht (N) wird per Funk empfangen. Eine per Funk ausgestrahlte zweite Einmalkennung (EK2) wird unabhängig von der Nachricht (N) empfangen. Die Nachricht (N) wird abhängig von der ersten Einmalkennung (EK1) und der zweiten Einmalkennung (EK2) auf ihre Gültigkeit überprüft. Die Nachricht (N) wird als gültig erkannt, wenn die erste Einmalkennung (EK1) und die zweite Einmalkennung (EK2) übereinstimmen oder wenn der erste Nachrichtenprüfwert (NP1) mit einem zweiten Nachrichtenprüfwert (NP2) übereinstimmt, der abhängig von der zweiten Einmalkennung (EK2) ermittelt wird, oder wenn eine abhängig von der zweiten Einmalkennung (EK2) ermittelte dritte Einmalkennung (EK3) mit der ersten Einmalkennung (EK1) übereinstimmt. Andernfalls wird die Nachricht (N) als ungültig erkannt.

FIG 7



EP 1 975 900 A2

Beschreibung

[0001] Prüfverfahren, Prüfvorrichtung, Sendeverfahren zum Aussenden von Nachrichten, Sendevorrichtung, Sendeverfahren zum Aussenden von Einmalkennungen, Sendestation und System

[0002] Die Erfindung betrifft ein Prüfverfahren und eine Prüfvorrichtung zum Überprüfen einer Nachricht. Die Erfindung betrifft ferner ein Sendeverfahren und eine Sendevorrichtung zum Aussenden einer Nachricht. Die Erfindung betrifft ferner ein Sendeverfahren und eine Sendestation zum Aussenden von Einmalkennungen. Die Erfindung betrifft ferner ein System.

[0003] Durch Fahrzeuge erfasste Daten sind per Funk als Nachrichten an andere Fahrzeuge übertragbar. Die Nachrichten umfassen zum Beispiel eine Glatteis- oder Unfallwarnung. Die Nachrichten sind beispielsweise von Fahrzeug zu Fahrzeug mit einer begrenzten Anzahl von Übertragungen, das heißt Sprüngen oder so genannten "Hops", übertragbar. Ein derartiges Übertragen von Nachrichten wird auch Fluten oder "Flooding" genannt. Es soll verhindert werden, dass die Nachrichten manipuliert oder wieder eingespielt werden können. Dazu muss ein jeweiliger Empfänger der Nachricht diese überprüfen können.

[0004] Die Aufgabe der Erfindung ist, ein Prüfverfahren, eine Prüfvorrichtung, ein Sendeverfahren zum Aussenden von Nachrichten, eine Sendevorrichtung, ein Sendeverfahren zum Aussenden von Einmalkennungen, eine Sendestation und ein System zu schaffen, das beziehungsweise die ein einfaches und zuverlässiges Überprüfen von Nachrichten ermöglicht.

[0005] Die Aufgabe wird gelöst durch die Merkmale der unabhängigen Patentansprüche. Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen gekennzeichnet.

[0006] Gemäß einem ersten Aspekt zeichnet sich die Erfindung aus durch ein Prüfverfahren und eine zugehörige Prüfvorrichtung zum Überprüfen einer Nachricht, die eine erste Einmalkennung oder einen abhängig von der ersten Einmalkennung ermittelten ersten Nachrichtenprüfwert umfasst. Die Nachricht wird per Funk empfangen. Eine per Funk ausgestrahlte zweite Einmalkennung wird unabhängig von der Nachricht empfangen. Die Nachricht wird abhängig von der ersten Einmalkennung und der zweiten Einmalkennung auf ihre Gültigkeit überprüft. Die Nachricht wird als gültig erkannt, wenn die erste Einmalkennung und die zweite Einmalkennung übereinstimmen oder wenn der erste Nachrichtenprüfwert mit einem zweiten Nachrichtenprüfwert übereinstimmt, der abhängig von der zweiten Einmalkennung ermittelt wird, oder wenn eine abhängig von der zweiten Einmalkennung ermittelte dritte Einmalkennung mit der ersten Einmalkennung übereinstimmt. Andernfalls wird die Nachricht als ungültig erkannt.

[0007] Die erste und die zweite Einmalkennung sind beispielsweise als Nonce und insbesondere als kryptographische Nonce ausgebildet. Eine solche Nonce ist beispielsweise eine Zahlen- und/oder Buchstabenkombination, die für eine einmalige Verwendung bestimmt ist und zum Beispiel als Zufallszahl oder Pseudozufallszahl ausgebildet ist. Die erste und die zweite Einmalkennung weisen insbesondere eine zeitlich und räumlich begrenzte Gültigkeit auf. Die räumliche Gültigkeit ist beispielsweise durch einen Empfangsbereich der per Funk ausgestrahlten Einmalkennung vorgegeben, kann jedoch auch anders vorgegeben sein. Die zeitliche Gültigkeit ergibt sich beispielsweise durch eine Änderung der per Funk ausgestrahlten Einmalkennung in einem vorgegebenen Zeitintervall, so dass zu unterschiedlichen Zeiten unterschiedliche Einmalkennungen empfangbar sind.

[0008] Der Vorteil ist, dass ein jeweiliger Empfänger der Nachricht sehr einfach die Gültigkeit der Nachricht in Bezug den räumlichen und zeitlichen Gültigkeitsbereich und somit in Bezug auf die Aktualität und Relevanz der Nachricht überprüfen kann. Wenn der Absender der Nachricht und der Empfänger der Nachricht die gleiche Einmalkennung empfangen haben und der Absender seine Nachricht mit dieser Einmalkennung schützt, zum Beispiel in Form der ersten Einmalkennung oder des ersten Nachrichtenprüfwerts, dann ergibt die Übereinstimmung der ersten und der zweiten Einmalkennung oder des ersten und des zweiten Nachrichtenprüfwerts oder der dritten und der ersten Einmalkennung, dass sich der Absender der Nachricht in der Nähe aufhält, da dieser die gleiche Einmalkennung kennt wie der Empfänger, und die Nachricht daher relevant sein kann und dass die Nachricht aktuell ist, das heißt, die Nachricht noch nicht veraltet ist.

[0009] Auf diese Weise ist ein einfacher und zuverlässiger Schutz vor Wiedereinspielangriffen, so genannten Replay-Angriffen, und vor so genannten Wormhole-Angriffen möglich. Bei Wormhole-Angriffen werden Nachrichten unbefugt räumlich entfernt von ihrem Gültigkeitsgebiet verbreitet. Dadurch, dass die Einmalkennungen nur einen räumlich begrenzten Gültigkeitsbereich haben, können Nachrichten einfach als ungültig erkannt werden, wenn die erste Einmalkennung oder der erste Nachrichtenprüfwert der Nachricht von der durch den Empfänger der Nachricht empfangenen zweiten Einmalkennung beziehungsweise von dem durch den Empfänger ermittelten zweiten Nachrichtenprüfwert oder von der durch den Empfänger ermittelten dritten Einmalkennung abweicht. Absender und Empfänger befinden sich dann in unterschiedlichen geographischen Gebieten und empfangen unterschiedliche Einmalkennungen. Vorteilhaft ist ferner, dass für die Überprüfbarkeit der Nachricht keine synchronisierten Uhren oder Positionsermittlungseinheiten erforderlich sind. Dadurch ist das Überprüfen einfach und kostengünstig möglich.

[0010] Die Einmalkennungen, insbesondere die erste Einmalkennung und die zweite Einmalkennung, werden bevorzugt durch vertrauenswürdige Infrastruktureinheiten ausgestrahlt, zum Beispiel durch staatlich kontrollierte Sendestationen, die räumlich voneinander beabstandet angeordnet sind, zum Beispiel entlang oder in der

Nähe von Straßen. Die Nachricht umfasst insbesondere eine Verkehrsinformation, zum Beispiel eine Verkehrsflussinformation oder sicherheitsrelevante Verkehrsinformation. Die Nachricht ist beispielsweise durch eine der Sendestationen oder durch ein Fahrzeug ausgesendet worden. Die Prüfvorrichtung ist insbesondere in einem Fahrzeug und insbesondere einem Kraftfahrzeug angeordnet und ist ausgebildet, die mittels der Nachricht empfangenen Verkehrsinformationen gegebenenfalls einem Fahrer des Fahrzeugs mitzuteilen oder bei einer Routenplanung zu berücksichtigen.

[0011] In einer vorteilhaften Ausgestaltung wird eine geographische Gebietsinformation zu der ersten Einmalkennung und/oder zu der zweiten Einmalkennung ermittelt. Ferner wird eine aktuelle geographische Position eines dieses Prüfverfahren aktuell ausführenden Empfängers der Nachricht, das heißt der Prüfvorrichtung, ermittelt. Die Nachricht wird abhängig von der geographischen Gebietsinformation und der ermittelten aktuellen geographischen Position auf ihre Gültigkeit überprüft. Die Nachricht wird als gültig erkannt, wenn die ermittelte aktuelle geographische Position innerhalb eines geographischen Gebiets liegt, das abhängig von der geographischen Gebietsinformation vorgegeben wird. Die Nachricht wird andernfalls als ungültig erkannt. Dies hat den Vorteil, dass die Überprüfung des Gültigkeitsgebiets besonders präzise und unabhängig von dem Empfangsbereich der Einmalkennung erfolgen kann.

[0012] In diesem Zusammenhang ist es vorteilhaft, wenn eine Anwendungsinformation zu der ersten Einmalkennung und/oder zu der zweiten Einmalkennung ermittelt wird und eine Größe des geographischen Gebiets abhängig von der Anwendungsinformation vorgegeben wird. Der Vorteil ist, dass für unterschiedliche Anwendungen sehr einfach unterschiedlich große geographische Gebiete vorgegeben werden können. Zum Beispiel kann für Verkehrsflussinformationen wie Baustelleninformationen, Stauinformationen oder Informationen über Straßensperrungen ein größeres geographisches Gebiet vorgesehen sein als für sicherheitsrelevante Verkehrsinformationen wie Glatteis-, Unfall- oder Nebelwarnungen.

[0013] In einer weiteren vorteilhaften Ausgestaltung ist die geographische Gebietsinformation und/oder die Anwendungsinformation der ersten Einmalkennung und/oder der zweiten Einmalkennung beigefügt. Dies hat den Vorteil, dass die jeweilige Information somit unmittelbar zur Verfügung steht und so das Überprüfen der Nachricht besonders einfach erfolgen kann.

[0014] In einer weiteren vorteilhaften Ausgestaltung wird die geographische Gebietsinformation und/oder die Anwendungsinformation von einem Server abgerufen für die erste Einmalkennung und/oder für die zweite Einmalkennung. Der Server ist beispielsweise über eine Internetverbindung erreichbar oder ist über die jeweilige Sendestation erreichbar. Der Vorteil ist, dass so nur ein besonders geringes Datenvolumen je Einmalkennung empfangen werden muss, die Informationen jedoch bei Bedarf auf Anfrage an den Server zur Verfügung stehen. Die Informationen müssen so jedoch nicht immer mit der jeweiligen Einmalkennung ausgestrahlt werden.

[0015] In einer weiteren vorteilhaften Ausgestaltung ist der ersten Einmalkennung und/oder der zweiten Einmalkennung ein jeweiliger Kennungsprüfwert beigefügt, der abhängig von der ersten Einmalkennung beziehungsweise der zweiten Einmalkennung ermittelt wurde. Eine Gültigkeit der ersten Einmalkennung beziehungsweise der zweiten Einmalkennung wird abhängig von einem dem jeweiligen Empfänger der Nachricht bekannten Schlüssel und abhängig von der ersten Einmalkennung beziehungsweise der zweiten Einmalkennung überprüft. Die Nachricht wird nur dann als gültig erkannt, wenn die Gültigkeit der ersten Einmalkennung beziehungsweise der zweiten Einmalkennung festgestellt wurde. Dies hat den Vorteil, dass die Einmalkennung und somit auch die Nachricht zuverlässig überprüfbar ist.

[0016] In einer weiteren vorteilhaften Ausgestaltung wird die dritte Einmalkennung durch einmaliges oder mehrmaliges rekursives Anwenden einer vorgegebenen Rechenvorschrift abhängig von der zweiten Einmalkennung ermittelt. Dies hat den Vorteil, dass die erste Einmalkennung auch dann einfach überprüfbar ist, wenn die erste Einmalkennung der Nachricht nicht auch als zweite Einmalkennung empfangen wurde, jedoch eine ältere Einmalkennung zur Verfügung steht. Eine solche Überprüfung ist möglich, wenn die zeitlich aufeinander folgend ausgestrahlten Einmalkennungen nicht unabhängig voneinander sind, sondern einer Kennungsliste entnommen sind, die auch als "Hash-Chain" bezeichnet werden kann.

[0017] In einer weiteren vorteilhaften Ausgestaltung wird die als gültig erkannte Nachricht per Funk ausgesandt. Der Vorteil ist, dass die Nachricht sehr einfach weiter verbreitet werden kann und somit die Reichweite der Nachricht und insbesondere der Verkehrsinformation, die diese trägt, erhöht werden kann.

[0018] Gemäß einem zweiten Aspekt zeichnet sich die Erfindung aus durch ein Sendeverfahren und eine entsprechende Sendevorrichtung zum Aussenden einer Nachricht. Eine per Funk ausgestrahlte Einmalkennung wird empfangen. Der Nachricht wird die empfangene Einmalkennung oder ein Nachrichtenprüfwert, der abhängig von der empfangenen Einmalkennung ermittelt wird, hinzugefügt. Die Nachricht wird per Funk ausgesandt.

[0019] Die Einmalkennung ist beispielsweise als Nonce und insbesondere als kryptographische Nonce ausgebildet. Eine solche Nonce ist beispielsweise eine Zahlen- und/oder Buchstabenkombination, die für eine einmalige Verwendung bestimmt ist und zum Beispiel als Zufallszahl oder Pseudozufallszahl ausgebildet ist. Die Einmalkennung weist insbesondere eine zeitlich und räumlich begrenzte Gültigkeit auf. Die räumliche Gültigkeit ist beispielsweise durch einen Empfangsbereich der per Funk ausgestrahlten Einmalkennung vorgegeben, kann jedoch auch anders vorgegeben sein. Die zeitliche Gültigkeit ergibt sich beispielsweise durch eine Änderung der per Funk ausgestrahlten Einmalkennung in ei-

nem vorgegebenen Zeitintervall, so dass zu unterschiedlichen Zeiten unterschiedliche Einmalkennungen empfangbar sind.

[0020] Der Vorteil ist, dass ein jeweiliger Empfänger der Nachricht sehr einfach die Gültigkeit der Nachricht in Bezug den räumlichen und zeitlichen Gültigkeitsbereich und somit in Bezug auf die Aktualität und Relevanz der Nachricht überprüfen kann. Wenn der Absender der Nachricht, das heißt die Sendevorrichtung, und der Empfänger der Nachricht die gleiche Einmalkennung empfangen haben und der Absender seine Nachricht mit dieser Einmalkennung schützt, zum Beispiel in Form der Einmalkennung oder des Nachrichtenprüfwerts, dann ergibt die Übereinstimmung der Einmalkennung oder des Nachrichtenprüfwerts der Nachricht mit der durch den Empfänger unabhängig von der Nachricht empfangenen Einmalkennung beziehungsweise dem durch den Empfänger abhängig von dieser Einmalkennung ermittelten Nachrichtenprüfwert, dass sich der Absender der Nachricht, das heißt die Sendevorrichtung, in der Nähe des Empfängers aufhält, da dieser die gleiche Einmalkennung kennt wie der Absender, und die Nachricht daher relevant sein kann und dass die Nachricht aktuell ist, das heißt, die Nachricht noch nicht veraltet ist.

[0021] Auf diese Weise ist ein einfacher und zuverlässiger Schutz vor Wiedereinspielangriffen, so genannten Replay-Angriffen, und vor so genannten Wormhole-Angriffen möglich. Bei Wormhole-Angriffen werden Nachrichten unbefugt räumlich entfernt von ihrem Gültigkeitsgebiet verbreitet. Dadurch, dass die Einmalkennungen nur einen räumlich begrenzten Gültigkeitsbereich haben, können Nachrichten durch den jeweiligen Empfänger der Nachricht einfach als ungültig erkannt werden, wenn die Einmalkennung der Nachricht oder der zugehörige Nachrichtenprüfwert der Nachricht von der durch den Empfänger der Nachricht empfangenen Einmalkennung beziehungsweise von dem durch den Empfänger ermittelten Nachrichtenprüfwert abweicht. Absender und Empfänger befinden sich dann in unterschiedlichen geographischen Gebieten und empfangen unterschiedliche Einmalkennungen. Vorteilhaft ist ferner, dass für die Überprüfbarkeit der Nachricht durch den jeweiligen Empfänger keine synchronisierten Uhren oder Positionsermittlungseinheiten erforderlich sind. Dadurch ist das Überprüfen einfach und kostengünstig möglich.

[0022] Die Einmalkennungen werden bevorzugt durch vertrauenswürdige Infrastruktureinheiten ausgestrahlt, zum Beispiel durch staatlich kontrollierte Sendestationen, die räumlich voneinander beabstandet angeordnet sind, zum Beispiel entlang oder in der Nähe von Straßen. Die Nachricht umfasst insbesondere eine Verkehrsinformation, zum Beispiel eine Verkehrsflussinformation oder sicherheitsrelevante Verkehrsinformation. Die Sendevorrichtung ist insbesondere in einem Fahrzeug und insbesondere einem Kraftfahrzeug angeordnet, kann jedoch ebenso in einer Sendestation angeordnet sein.

[0023] Gemäß einem dritten Aspekt zeichnet sich die Erfindung aus durch ein Sendeverfahren und eine entsprechende Sendestation zum Aussenden von Einmalkennungen. Jeweils mindestens eine Einmalkennung wird in einem vorgegebenen Zeitintervall ermittelt, wobei die jeweilige Einmalkennung individuell und eindeutig für die Sendestation und für das jeweilige Zeitintervall ermittelt wird. Die jeweils mindestens eine Einmalkennung wird per Funk ausgestrahlt.

[0024] Die jeweils mindestens eine Einmalkennung wird insbesondere per Rundfunk ausgestrahlt. Rundfunk bezeichnet die Übertragung von Informationen jeglicher Art über elektromagnetische Wellen, wobei die Informationen für die Öffentlichkeit gedacht sind und von jedermann empfangen werden können.

[0025] Die jeweilige Einmalkennung ist beispielsweise als Nonce und insbesondere als kryptographische Nonce ausgebildet. Eine solche Nonce ist beispielsweise eine Zahlen- und/oder Buchstabenkombination, die für eine einmalige Verwendung bestimmt ist und zum Beispiel als Zufallszahl oder Pseudozufallszahl ausgebildet ist. Die Einmalkennung weist insbesondere eine zeitlich und räumlich begrenzte Gültigkeit auf. Die räumliche Gültigkeit ist beispielsweise durch einen Empfangsbereich der per Funk ausgestrahlten Einmalkennung vorgegeben, kann jedoch auch anders vorgegeben sein. Da Sendestationen räumlich voneinander beabstandet angeordnet werden und die jeweilige Einmalkennung indiviuell und eindeutig für die jeweilige Sendestation ermittelt wird, ist durch die jeweilige Einmalkennung eine räumliche Zuordnung zu der jeweiligen Sendestation gegeben. Die zeitliche Gültigkeit ergibt sich durch eine Änderung der per Funk ausgestrahlten Einmalkennung in dem vorgegebenen Zeitintervall, so dass zu unterschiedlichen Zeiten unterschiedliche Einmalkennungen empfangbar sind.

[0026] Der Vorteil ist, dass die jeweilige Einmalkennung genutzt werden kann, um Nachrichten zu schützen und überprüfbar zu machen. Ein jeweiliger Empfänger der Nachricht kann sehr einfach die Gültigkeit der Nachricht in Bezug auf den räumlichen und zeitlichen Gültigkeitsbereich und somit in Bezug auf die Aktualität und Relevanz der Nachricht überprüfen. Wenn der Absender der Nachricht und der Empfänger der Nachricht die gleiche Einmalkennung empfangen haben und der Absender seine Nachricht mit dieser Einmalkennung schützt, zum Beispiel in Form der Einmalkennung oder eines Nachrichtenprüfwerts, dann ergibt die Übereinstimmung der Einmalkennung oder des Nachrichtenprüfwerts der Nachricht mit der durch den Empfänger unabhängig von der Nachricht empfangenen Einmalkennung beziehungsweise dem durch den Empfänger abhängig von dieser Einmalkennung ermittelten Nachrichtenprüfwert, dass sich der Absender der Nachricht in der Nähe des Empfängers aufhält, da dieser die gleiche Einmalkennung kennt wie der Absender, und die Nachricht daher relevant sein kann und dass die Nachricht aktuell ist, das heißt, die Nachricht noch nicht veraltet ist.

[0027] Auf diese Weise ist ein einfacher und zuverlässiger Schutz vor Wiedereinspielangriffen, so genannten

Replay-Angriffen, und vor so genannten Wormhole-Angriffen möglich. Bei Wormhole-Angriffen werden Nachrichten unbefugt räumlich entfernt von ihrem Gültigkeitsgebiet verbreitet. Dadurch, dass die Einmalkennungen nur einen räumlich begrenzten Gültigkeitsbereich haben, können Nachrichten durch den jeweiligen Empfänger der Nachricht einfach als ungültig erkannt werden, wenn die Einmalkennung der Nachricht oder der zugehörige Nachrichtenprüfwert der Nachricht von der durch den Empfänger der Nachricht empfangenen Einmalkennung beziehungsweise von dem durch den Empfänger ermittelten Nachrichtenprüfwert abweicht. Absender und Empfänger befinden sich dann in unterschiedlichen geographischen Gebieten und empfangen unterschiedliche Einmalkennungen. Vorteilhaft ist ferner, dass für die Überprüfbarkeit der Nachricht durch den jeweiligen Empfänger keine synchronisierten Uhren oder Positionsermittlungseinheiten erforderlich sind. Dadurch ist das Überprüfen einfach und kostengünstig möglich.

[0028] Die Sendestation ist vorzugsweise eine vertrauenswürdige Infrastruktureinheit, die zum Beispiel staatlich kontrolliert wird. Sendestationen sind beispielsweise räumlich voneinander beabstandet angeordnet, zum Beispiel entlang oder in der Nähe von Straßen. Die Nachricht umfasst insbesondere eine Verkehrsinformation, zum Beispiel eine Verkehrsflussinformation oder sicherheitsrelevante Verkehrsinformation. Die Sendestation weist ferner eine Zeitmesseinheit zum Vorgeben des vorgegebenen Zeitintervalls und eine Sendeeinheit zum Ausstrahlen der jeweiligen Einmalkennung auf.

[0029] In einer vorteilhaften Ausgestaltung des dritten Aspekts wird die jeweilige Einmalkennung ermittelt durch Auswahl eines jeweils nächsten Listeneintrags einer Kennungsliste, deren Listeneinträge jeweils erzeugt werden durch rekursives Anwenden einer vorgegebenen Rechenvorschrift abhängig von einer vorgegebenen Anfangskennung. Eine solche Kennungsliste kann auch als "Hash-Chain" bezeichnet werden. Auf diese Weise sind die Einmalkennungen einfach und zuverlässig ermittelbar und sind durch einen Empfänger der jeweiligen Einmalkennung einfach überprüfbar, wenn dieser bereits über eine ältere Einmalkennung der Kennungsliste verfügt, die bereits früher ausgestrahlt wurde.

[0030] In einer weiteren vorteilhaften Ausgestaltung des dritten Aspekts wird die jeweilige Einmalkennung ermittelt als ein Zufallswert oder Pseudozufallswert. Dies ist besonders einfach.

[0031] In einer weiteren vorteilhaften Ausgestaltung des dritten Aspekts wird die jeweils ermittelte Einmalkennung für eine vorgegebene Zeitdauer wiederholt ausgesandt, die länger ist als das vorgegebene Zeitintervall. Dadurch ergibt sich eine zeitliche Überlappung der Gültigkeit von aufeinander folgenden Einmalkennungen. Dadurch ist eine höhere Zuverlässigkeit bei wechselnden Empfangsbedingungen möglich. Ferner sind so auch etwas ältere Nachrichten noch überprüfbar.

[0032] In einer weiteren vorteilhaften Ausgestaltung des dritten Aspekts wird mindestens eine Einmalkennung von einer benachbarten Sendestation empfangen und zusätzlich ausgestrahlt. Dadurch ergibt sich eine räumliche Überlappung der Gültigkeit von Einmalkennungen. Dadurch ist eine höhere Zuverlässigkeit bei wechselnden Empfangsbedingungen möglich.

[0033] In einer weiteren vorteilhaften Ausgestaltung des dritten Aspekts werden Nachrichten empfangen, überprüft und gegebenenfalls ausgesandt, wobei die jeweilige Nachricht eine erste Einmalkennung oder einen abhängig von der ersten Einmalkennung ermittelten ersten Nachrichtenprüfwert umfasst und das Überprüfen der jeweiligen Nachricht abhängig von der ersten Einmalkennung und mindestens einer der Einmalkennungen der Sendestation und/oder der benachbarten Sendestation durchgeführt wird. Die jeweilige Nachricht wird nur dann ausgesandt, wenn die erste Einmalkennung und die mindestens eine der Einmalkennungen der Sendestation oder der benachbarten Sendestation übereinstimmen oder wenn der erste Nachrichtenprüfwert mit einem zweiten Nachrichtenprüfwert übereinstimmt, der abhängig von der mindestens einen der Einmalkennungen der Sendestation und/oder der benachbarten Sendestation ermittelt wird. Dies hat den Vorteil, dass die Nachrichten eine größere Reichweite haben können.

[0034] In einer weiteren vorteilhaften Ausgestaltung des dritten Aspekts wird der jeweiligen Einmalkennung eine geographische Gebietsinformation und/oder eine Anwendungsinformation und/oder eine Gültigkeitsdauer beigefügt. Dadurch ist eine besonders präzise Überprüfung des räumlichen und/oder zeitlichen Gültigkeitsbereichs unabhängig von dem Empfangsbereich der Einmalkennung möglich. Ferner können für unterschiedliche Anwendungen sehr einfach unterschiedlich große geographische Gebiete vorgegeben werden, zum Beispiel für Verkehrsflussinformationen ein größeres geographisches Gebiet als für sicherheitsrelevante Verkehrsinformationen.

[0035] In einer weiteren vorteilhaften Ausgestaltung des dritten Aspekts wird der jeweiligen Einmalkennung ein jeweiliger Kennungsprüfwert beigefügt, der abhängig von der jeweiligen Einmalkennung ermittelt wird. Dies hat den Vorteil, dass die jeweilige Einmalkennung einfach und zuverlässig überprüfbar ist.

[0036] Gemäß einem vierten Aspekt zeichnet sich die Erfindung aus durch ein System, das mindestens zwei Sendestationen gemäß dem dritten Aspekt und mindestens zwei Prüf- und/oder Sendevorrichtungen gemäß dem ersten beziehungsweise dem zweiten Aspekt umfasst. Vorteilhafte Ausgestaltungen und Vorteile des Systems entsprechen denen des ersten bis dritten Aspekts.

[0037] Ausführungsbeispiele der Erfindung sind im Folgenden anhand der schematischen Zeichnungen erläutert. Es zeigen:

Figur 1 ein Senden und Weiterleiten von Einmalkennungen zwischen Sendestationen und Fahrzeugen,

Figur 2 ein Senden und Weiterleiten von Nachrichten zwischen Sendestationen und Fahrzeugen,

Figur 3 durch verschiedene Sendestationen abgedeckte geographische Gebiete,

Figur 4 ein schematischer Aufbau einer Nachricht,

Figur 5 ein Ablaufdiagramm eines Programms zum Aussenden von Einmalkennungen,

Figur 6 ein Ablaufdiagramm eines Programms zum Aussenden von Nachrichten und

Figur 7 ein Ablaufdiagramm eines Programms zum Prüfen von empfangenen Nachrichten.

[0038] Elemente gleicher Konstruktion oder Funktion sind figurenübergreifend mit den gleichen Bezugszeichen versehen.

[0039] Ein System umfasst mindestens eine erste Sendestation STAT1 und eine zweite Sendestation STAT2 und mindestens zwei Prüfvorrichtungen PV und/oder Sendevorrichtungen SV (Figuren 1 und 2). Die Sendestationen sind räumlich voneinander beabstandet angeordnet, zum Beispiel entlang einer Straße. Der Abstand der Sendestationen beträgt vorzugsweise einige 10 Meter, einige 100 Meter oder auch einen oder mehrere Kilometer. Vorzugsweise sind die Sendestationen in einer Stadt dichter beieinander angeordnet, das heißt zum Beispiel in einem Abstand von einigen 10 oder wenigen 100 Metern, als außerhalb der Stadt, wo diese in einem Abstand von einigen 100 Metern oder Kilometern angeordnet sein können. Vorzugsweise sind die Sendestationen stationär ausgebildet, das heißt ortsfest. Die Sendestationen können jedoch ebenso mobil ausgebildet sein und zum Beispiel auf einem Fahrzeug angeordnet sein. Die Sendestationen umfassen jeweils eine Sendeeinheit SE und eine Zeitmesseinheit ZME.

[0040] Die Sendestationen sind ausgebildet, Einmalkennungen EK auszustrahlen, die eine räumlich und zeitlich begrenzte Gültigkeit aufweisen. In einem vorgegebenen Zeitintervall ZI, das mittels der Zeitmesseinheit ZME vorgegeben wird, ermittelt die jeweilige Sendestation eine jeweils individuelle und eindeutige Einmalkennung EK und strahlt diese mittels der Sendeeinheit SE per Funk aus. Beispielsweise strahlt die erste Sendestation STAT1 eine Einmalkennung EK_GEO1 für ein erstes geographisches Gebiet GEO1 aus. Entsprechend sendet die zweite Sendestation STAT2 eine Einmalkennung EK_GE02 für ein zweites geographisches Gebiet GE02 aus. Die Einmalkennung EK_GE01 für das erste geographische Gebiet GEO1 und die Einmalkennung EK_GE02 für das zweite geographische Gebiet GE02 unterscheiden sich voneinander. Die Einmalkennungen EK sind beispielsweise als Nonce und insbesondere als kryptographische Nonce ausgebildet. Eine solche kryptographische Nonce ist beispielsweise eine Zahlen- und/oder Buchstabenkombination für eine einmalige Verwendung. Eine solche Nonce ist beispielsweise als eine Zufallszahl oder als eine Pseudozufallszahl ausgebildet, kann jedoch auch anders ausgebildet sein, zum Beispiel als eine fortlaufende Nummer.

[0041] Die Prüfvorrichtung PV und/oder die Sendevorrichtung SV sind vorzugsweise gemeinsam in einer Einheit ausgebildet und in einem Fahrzeug angeordnet. In Figuren 1 und 2 sind beispielsweise ein erstes Fahrzeug F1, ein zweites Fahrzeug F2, ein drittes Fahrzeug F3, ein viertes Fahrzeug F4 und ein fünftes Fahrzeug F5 abgebildet, die jeweils die Prüfvorrichtung PV und/oder die Sendevorrichtung SV umfassen. Die Prüfvorrichtung PV und die Sendevorrichtung SV sind ausgebildet, die Einmalkennungen EK zu empfangen, die durch die jeweiligen Sendestationen ausgestrahlt werden. Aufgrund der begrenzten Reichweite der Sendestationen können die jeweils zugehörigen Einmalkennungen EK nur in einem begrenzten Empfangsgebiet um die jeweilige Sendestation direkt empfangen werden. Es kann jedoch auch vorgesehen sein, die empfangenen Einmalkennungen EK an andere Fahrzeuge weiterzusenden, um so das Empfangsgebiet für die jeweilige Einmalkennung EK zu vergrößern. Vorzugsweise ist eine Anzahl der Weiterversendungen an andere Fahrzeuge begrenzt, so dass auch das Verbreitungsgebiet für die jeweilige Einmalkennung EK begrenzt bleibt.

[0042] In dem in Figur 1 gezeigten Beispiel empfangen das erste Fahrzeug F1, das zweite Fahrzeug F2 und das dritte Fahrzeug F3 jeweils die Einmalkennung EK_GE01 für das erste geographische Gebiet GE01. Das vierte Fahrzeug F4 empfängt die Einmalkennung EK_GE02 für das zweite geographische Gebiet GE02. Das zweite Fahrzeug F2 sendet die von ihm empfangene Einmalkennung EK_GEO1 für das erste geographische Gebiet GEO1 an das fünfte Fahrzeug F5 und dieses sendet diese weiter zu dem vierten Fahrzeug F4. Das vierte Fahrzeug F4 sendet die von ihm empfangene Einmalkennung EK_GE02 für das zweite geographische Gebiet GE02 an das dritte Fahrzeug F3 und das fünfte Fahrzeug F5. Ferner sendet das dritte Fahrzeug F3 die von ihm empfangene Einmalkennung EK_GEO1 für das erste geographische Gebiet GEO1 ebenfalls an das vierte Fahrzeug F4.

[0043] Figur 2 zeigt das Aussenden von Nachrichten N durch die Sendestationen und die Fahrzeuge. Die Nachrichten N umfassen beispielsweise Verkehrsflussinformationen oder sicherheitsrelevante Verkehrsinformationen. Zu den Verkehrsflussinformationen gehören beispielsweise Stauwarnungen, Hinweise auf Baustellen oder Straßensperrungen und dergleichen. Die sicherheitsrelevanten Verkehrsinformationen umfassen beispielsweise Glatteiswarnungen, Unfallwarnungen oder Nebelwarnungen. Bevorzugt werden solche Nachrichten N von Fahrzeug zu Fahrzeug weiter versandt und auf diese Weise verbreitet. Eine solche Art der Verbreitung von Nachrichten N wird auch Fluten oder "Flooding" genannt. Ferner können solche Nachrichten N auch durch

die Sendestationen empfangen und wieder ausgesandt werden. Auf diese Weise ist sichergestellt, dass eine große Anzahl von Fahrzeugen in dem geographischen Gebiet GEO der jeweiligen Sendestation und gegebenenfalls angrenzenden geographischen Gebieten GEO die Nachrichten N erhalten können.

[0044] In dem in Figur 2 gezeigten Beispiel sendet das vierte Fahrzeug F4 eine Nachricht N aus, die durch die zweite Sendestation STAT2 und das dritte Fahrzeug F3 empfangen wird. Das dritte Fahrzeug F3 sendet diese Nachricht N oder eine eigene Nachricht N an die erste Sendestation STAT1. Die erste Sendestation STAT1 sendet diese Nachricht N wieder aus. Die durch die erste Sendestation STAT1 ausgesandte Nachricht N wird durch das erste Fahrzeug F1 und durch das zweite Fahrzeug F2 empfangen. Das zweite Fahrzeug F2 sendet diese oder eine eigene Nachricht N aus, die durch das fünfte Fahrzeug F5 empfangen wird.

[0045] Um Manipulationen der Nachrichten N vorzubeugen und um eine Aktualität der Nachrichten N und eine Relevanz für das jeweilige geographische Gebiet GEO zu bewirken, umfasst die jeweilige Nachricht N die Einmalkennung EK des ursprünglichen Absenders der Nachricht N oder einen abhängig von dieser Einmalkennung EK ermittelten Nachrichtenprüfwert NP. Der jeweilige Empfänger der Nachricht N kann die Nachricht abhängig von der Einmalkennung EK, die in der Nachricht N kodiert ist, oder dem Nachrichtenprüfwert NP und abhängig von der selbst und unabhängig von der Nachricht N empfangenen Einmalkennung EK überprüfen.

[0046] Bevorzugt ist der Einmalkennung EK ein Kennungsprüfwert KP beigefügt, der abhängig von der Einmalkennung EK ermittelt wurde. Der Kennungsprüfwert KP ist beispielsweise als eine digitale Signatur ausgebildet und ist durch einen Schlüssel überprüfbar, der dem jeweiligen Empfänger der Einmalkennung EK oder der Nachricht N bekannt ist. Durch den Kennungsprüfwert KP kann die Authentizität der Einmalkennung EK überprüft werden. Der Kennungsprüfwert KP kann jedoch auch anders ausgebildet sein.

[0047] Für die jeweilige Einmalkennung EK können auch weitere Informationen vorgesehen sein, die dieser beigefügt sind und mit dieser ausgestrahlt werden oder die durch Anfrage an einen Server SERV anforderbar sind. Beispielsweise ist eine geographische Gebietsinformation GEO_INF vorgesehen, die einen räumlichen Gültigkeitsbereich der jeweiligen Einmalkennung EK beschreibt. Beispielsweise ist die geographische Gebietsinformation GEO_INF als ein vorgegebener Umkreis um den jeweiligen Standort der die jeweilige Einmalkennung EK ausstrahlenden Sendestation vorgegeben. Die geographische Gebietsinformation GEO_INF kann jedoch auch anders vorgegeben sein.

[0048] Ferner kann eine Anwendungsinformation ANW_INF vorgesehen sein, die einen Anwendungsbereich der jeweiligen Einmalkennung EK vorgibt. Beispielsweise ermöglicht die Anwendungsinformation ANW_INF eine Unterscheidung in Verkehrsflussinformationen und in sicherheitsrelevante Verkehrsinformationen. Beispielsweise ist das geographische Gebiet GEO, in der die jeweilige Einmalkennung EK Gültigkeit besitzt, abhängig von der Anwendungsinformation ANW_INF vorgegeben. Beispielsweise ist vorgesehen, dass eine Größe des geographischen Gebiets GEO für Verkehrsflussinformationen größer ist als für sicherheitsrelevante Verkehrsinformationen. Das jeweilige geographische Gebiet GEO kann jedoch auch anders vorgegeben sein.

[0049] Figur 3 zeigt eine Draufsicht auf drei Sendestationen, die erste Sendestation STAT1, die zweite Sendestation STAT2 und eine dritte Sendestation STAT3. Für jede der Sendestationen ist das zugehörige geographische Gebiet GEO in Form eines Kreises um den Standort der jeweiligen Sendestation gekennzeichnet. Das erste geographische Gebiet GEO1 ist der ersten Sendestation STAT1 zugeordnet, das zweite geographische Gebiet GE02 ist der zweiten Sendestation STAT2 zugeordnet und ein drittes geographisches Gebiet GE03 ist der dritten Sendestation STAT3 zugeordnet. In dem in Figur 3 gezeigten Beispiel sind das erste und das zweite geographische Gebiet GE01, GE02 einander überlappend vorgegeben. Durch das räumliche Überlappen der geographischen Gebiete GEO wird erreicht, dass in einem Überlappungsgebiet sowohl die jeweilige Einmalkennung EK_GEO1 für das erste geographische Gebiet GEO1 der ersten Sendestation STAT1 als auch die jeweilige Einmalkennung EK_GEO2 für das zweite geographischen Gebiet GE02 der zweiten Sendestation STAT2 gültig ist. So findet kein abrupter Wechsel der Einmalkennungen EK in den aneinander grenzenden Gebieten statt, wenn das jeweilige Fahrzeug von einem der geographischen Gebiete GEO in ein benachbartes geographisches Gebiet GEO fährt. Die geographischen Gebiete GEO können jedoch auch ohne Überlapung vorgegeben sein, wie in Figur 3 beispielhaft für das dritte geographische Gebiet GE03 dargestellt ist. Ferner kann vorgesehen sein, dass Sendestationen auch Einmalkennungen EK benachbarter Sendestationen zusätzlich aussenden, um so das Empfangsgebiet für die jeweilige Einmalkennung EK zu vergrößern und den Übergang von dem einen geographischen Gebiet GEO in das benachbarte geographische Gebiet GEO zu vereinfachen.

[0050] Entsprechend der räumlichen Überlappung der geographischen Gebiete GEO kann auch vorgesehen sein, die Gültigkeitsdauer der jeweiligen Einmalkennung EK in dem jeweiligen geographischen Gebiet GEO einander überlappend auszubilden, so dass jeweils mindestens zwei Einmalkennungen EK gleichzeitig in dem jeweiligen geographischen Gebiet GEO gültig sind. Dadurch steht immer auch eine etwas ältere gültige Einmalkennung EK zur Verfügung, mit deren Hilfe auch etwas ältere Nachrichten N überprüfbar sind.

[0051] In jedem der geographischen Gebiete GEO ist eine andere, für das jeweilige geographische Gebiet GEO und die jeweilige Gültigkeitsdauer eindeutige Einmalkennung EK gültig. In dem ersten geographischen

Gebiet GEO ist die Einmalkennung EK_GEO1 für das erste geographische Gebiet GEO1 gültig, in dem zweiten geographischen Gebiet GE02 ist die Einmalkennung für das zweite geographische Gebiet GE02 gültig und in dem dritten geographischen Gebiet GE03 ist eine Einmalkennung EK_GE03 für das dritte geographische Gebiet GE03 gültig.

[0052] Figur 4 zeigt einen beispielhaften Aufbau einer Nachricht N umfassend mehrere Felder unterschiedlichen Inhalts. Die Nachricht N umfasst Daten DAT, die auch als Nutzdaten bezeichnet werden können. Die Daten DAT umfassen beispielsweise die Verkehrsflussinformation oder die sicherheitsrelevante Verkehrsinformation. Vorzugsweise weist die Nachricht N auch eine Senderkennung SID auf, so dass der Absender der Nachricht N identifizierbar ist.

[0053] Ferner umfasst die Nachricht N die Einmalkennung EK des Absenders der Nachricht N und/oder den abhängig von der Einmalkennung EK des Absenders ermittelten Nachrichtenprüfwert NP. Der Nachrichtenprüfwert NP kann beispielsweise in Form eines Nachrichtenauthentisierungskodes, der auch als "Message Authentication Code", oder kurz: MAC, bezeichnet werden kann, ermittelt werden. Beispielsweise kann die Einmalkennung EK als Schlüssel für das Ermitteln des Nachrichtenprüfwertes NP genutzt werden. Der Nachrichtenprüfwert NP wird beispielsweise abhängig von den Daten DAT und gegebenenfalls auch abhängig von der Senderkennung SID und/oder weiteren Feldern der Nachricht N gebildet. Auf diese Weise ist eine Manipulation der Nachricht N feststellbar. Ferner ist überprüfbar, ob eine gültige Einmalkennung EK für das Ermitteln des Nachrichtenprüfwerts NP genutzt wurde, wenn der jeweilige Empfänger der Nachricht N ebenfalls die Einmalkennung EK kennt, die für das Ermitteln des Nachrichtenprüfwerts NP genutzt wurde.

[0054] Es kann jedoch unabhängig von der Einmalkennung EK auch ein weiterer Nachrichtenprüfwert in der Nachricht N vorgesehen sein, der beispielsweise ausgebildet ist als ein Fehlerprüfwert, zum Beispiel entsprechend einem "Cyclic Redundancy Check" oder kurz: CRC, oder als Nachrichtenauthentisierungskode, zum Beispiel entsprechend einem AES-CBC-MAC oder HMAC-SHA1, oder als digitale Signatur, zum Beispiel als RSA-Signatur nach PKCS#1 oder als DSA-Signatur. Der weitere Nachrichtenprüfwert kann sich auf alle Felder der Nachricht N beziehen, abgesehen von dem Feld, das den weiteren Nachrichtenprüfwert umfasst, oder kann sich einen Teil der Felder der Nachricht N beziehen, zum Beispiel auf die Daten DAT und die Senderkennung SID.

[0055] In der Nachricht N können ferner auch die gegebenenfalls der Einmalkennung EK beigefügten weiteren Informationen, also beipielsweise die geographische Gebietsinformation GEO_INF und/oder die Anwendungsinformation ANW_INF und/oder der Kennungsprüfwert KP, enthalten sein. Die Nachricht N kann auch weitere Informationen oder Daten umfassen. Ferner kann auch eine Reihenfolge der Informationen und Daten in der Nachricht N eine andere sein als in der Figur 4 dargestellt.

[0056] Figur 5 zeigt ein Ablaufdiagramm eines Programms zum Aussenden von Einmalkennungen EK durch die jeweilige Sendestation. Das Programm beginnt in einem Schritt S1. In einem Schritt S2 wird jeweils mindestens eine Einmalkennung EK in einem vorgegebenen Zeitintervall ZI ermittelt. Die jeweils ermittelte Einmalkennung EK wird individuell und eindeutig für die jeweilige Sendestation und für das jeweilige Zeitintervall ermittelt. Das vorgegebene Zeitintervall ZI weist bevorzugt eine Größenordnung von Sekunden oder Minuten auf. Das vorgegebene Zeitintervall ZI kann jedoch je nach Bedarf auch anders vorgegeben sein.

[0057] Die Einmalkennung EK wird vorzugsweise als Nonce und insbesondere als kryptographische Nonce ermittelt, zum Beispiel als Zufallszahl, Pseudozufallszahl oder auch als ein Element einer so genannten "Hash-Chain". Eine solche "Hash-Chain" ist eine Kennungsliste, deren Listeneinträge jeweils eine Einmalkennung umfassen. Die Listeneinträge der Kennungsliste werden ausgehend von einer vorgegebenen Anfangskennung durch rekursives Anwenden einer vorgegebenen Rechenvorschrift ermittelt. Diese vorgegebene Rechenvorschrift repräsentiert eine nicht umkehrbare mathematische Operation, so dass aufeinander folgende Listeneinträge, also Einmalkennungen EK, nur in einer Richtung von der vorgegebenen Anfangskennung weg berechenbar sind. Durch Anwenden der vorgegebenen Rechenvorschrift kann zwar von jedem beliebigen Listeneintrag aus ein Listeneintrag berechnet werden, der einen größeren Abstand zu der vorgegebenen Anfangskennung aufweist, nicht jedoch ein Listeneintrag, der einen geringeren Abstand zu der vorgegebenen Anfangskennung aufweist. Ein großer Abstand zu der vorgegebenen Anfangskennung im Vergleich zu einem geringen Abstand bedeutet dabei, das die vorgegebene Rechenvorschrift häufiger rekursiv angewendet wurde.

[0058] Bei dem Ermitteln der jeweiligen Einmalkennung EK aus einer solchen Kennungsliste wird dann der jeweils nächste Listeneintrag ausgewählt, der einen geringeren Abstand zu der vorgegebenen Anfangskennung aufweist. Die Kennungsliste und insbesondere die Anfangskennung sind vorzugsweise nur der jeweiligen Sendestation bekannt, nicht jedoch der jeweiligen Prüfvorrichtung PV in den Fahrzeugen. Jedoch ist vorzugsweise die vorgegebene Rechenvorschrift auch den Prüfvorrichtungen PV bekannt. Auf diese Weise ist eine jüngere Einmalkennung EK anhand einer älteren Einmalkennung EK überprüfbar, zum Beispiel durch die Prüfvorrichtung PV des jeweiligen Empfängers, wenn die jüngere und die ältere Einmalkennung EK aus der gleichen Kennungsliste stammen. Für das Überprüfen muss die vorgegebene Rechenvorschrift einmal oder mehrmals rekursiv auf die jüngere Einmalkennung EK angewendet werden, um als Ergebnis die ältere Einmalkennung EK zu erhalten.

[0059] In einem dritten Schritt S3 wird gegebenenfalls die Einmalkennung EK' einer benachbarten Sendestation empfangen. In einem Schritt S4 kann vorgesehen sein, dass der ermittelten Einmalkennung EK die geographische Gebietsinformation GEO_INF und/oder die Anwendungsinformation ANW_INF oder auch andere Informationen, zum Beispiel bezüglich der zeitlichen Gültigkeit, beigefügt werden. Ferner kann der Kennungsprüfwert KP ermittelt werden und der ermittelten Einmalkennung EK beigefügt werden. In einem Schritt S5 wird die Einmalkennung EK gegebenenfalls zusammen mit der geographischen Gebietsinformation GEO_INF und/oder der Anwendungsinformation ANW_INF und/oder den weiteren Informationen und/oder dem Kennungsprüfwert KP ausgestrahlt. Ferner wird die gegebenenfalls empfangene Einmalkennung EK' der benachbarten Sendestation zusätzlich ausgestrahlt.

[0060] Ferner können weitere Schritte vorgesehen sein für das Empfangen, Überprüfen und gegebenenfalls Aussenden von Nachrichten N. In einem Schritt S6 ist dazu vorgesehen, dass Nachrichten N empfangen werden, die beispielsweise durch Fahrzeuge oder benachbarte Sendestationen ausgesandt werden. Es kann jedoch auch vorgesehen sein, Nachrichten N oder die zugehörigen Daten DAT von einer Verkehrsdateninfrastruktur zu empfangen, die diese Informationen zentral für mehere oder alle Sendestationen zur Verfügung stellt.

[0061] In einem Schritt S7 können die empfangenen Nachrichten N überprüft werden. Die jeweilige empfangene Nachricht N umfasst eine erste Einmalkennung EK1 des ursprünglichen Absenders der Nachricht N oder einen abhängig von der ersten Einmalkennung EK1 ermittelten ersten Nachrichtenprüfwert NP1. Das Überprüfen der jeweiligen Nachricht N erfolgt abhängig von der ersten Einmalkennung EK1 und mindestens einer der Einmalkennungen EK der Sendestation und/oder der benachbarten Sendestation. Gegebenenfalls wird ein jeweiliger zweiter Nachrichtenprüfwert NP2 abhängig von der jeweiligen Nachricht N und der Einmalkennung EK der Sendestation und/oder der benachbarten Sendestation ermittelt.

[0062] In einem Schritt S8 wird überprüft, ob die erste Einmalkennung EK1 und die mindestens eine der Einmalkennungen EK der Sendestation oder der benachbarten Sendestation übereinstimmen oder ob der erste Nachrichtenprüfwert NP1 mit dem zweiten Nachrichtenprüfwert NP2 übereinstimmt. Ist dies der Fall, dann kann die Nachricht N in einem Schritt S9 ausgesandt werden und das Programm in einem Schritt S10 beendet werden. Sind die Bedingungen in dem Schritt S8 jedoch nicht erfüllt, dann wird das Programm in dem Schritt S10 beendet. Vorzugsweise wird das Programm in dem Schritt S2 fortgesetzt, so dass die Einmalkennungen EK in dem vorgegebenen Zeitintervall ZI erzeugt werden. Das Ermitteln und Ausstrahlen der Einmalkennungen EK und das Empfangen, Überprüfen und Aussenden der Nachrichten N kann auch in einer anderen Reihenfolge und insbesondere auch parallel zueinander erfolgen.

[0063] Figur 6 zeigt ein Ablaufdiagramm eines Programms zum Aussenden von Nachrichten N. Das Programm wird beispielsweise durch die Sendevorrichtung SV ausgeführt. Das Programm beginnt in einem Schritt S11. In einem Schritt S12 wird die per Funk durch eine der Sendestationen ausgestrahlte Einmalkennung EK empfangen. Ein Schritt S13 kann vorgesehen sein zum Ermitteln des Nachrichtenprüfwerts NP abhängig von der zu versendenden Nachricht N und der empfangenen Einmalkennung EK. In einem Schritt S14 wird die Einmalkennung EK und/oder der ermittelte Nachrichtenprüfwert NP der Nachricht N hinzugefügt. In einem Schritt S15 wird die Nachricht N per Funk ausgesandt. Das Programm endet in einem Schritt S16 und wird beispielsweise für jede zu versendende Nachricht N wiederholt.

[0064] Figur 7 zeigt ein Ablaufdiagramm eines Programms zum Überprüfen von Nachrichten N, die eine erste Einmalkennung EK1 oder einen abhängig von der ersten Einmalkennung EK1 ermittelten ersten Nachrichtenprüfwert NP1 umfassen. Die erste Einmalkennung EK1 beziehungsweise der erste Nachrichtenprüfwert NP1 entsprechen dabei insbesondere der Einmalkennung EK beziehungsweise dem Nachrichtenprüfwert NP, die beziehungsweise der durch die Sendevorrichtung SV der jeweiligen Nachricht N gemäß dem in Figur 6 gezeigten Programm hinzugefügt wurde.

[0065] Das Programm beginnt in einem Schritt S20 und wird beispielsweise durch die Prüfvorrichtung PV ausgeführt. In einem Schritt S21 wird die jeweilige Nachricht N empfangen. In einem Schritt S22 wird eine per Funk ausgestrahlte zweite Einmalkennung EK2 unabhängig von der Nachricht N empfangen. Die empfangene zweite Einmalkennung EK2 entspricht insbesondere der Einmalkennung EK, die durch eine der Sendestationen gemäß dem in Figur 5 dargestellten Programm ausgestrahlt wird.

[0066] In einem Schritt S23 erfolgt das Überprüfen der Nachricht N abhängig von der ersten Einmalkennung EK1 und der zweiten Einmalkennung EK2. Für das Überprüfen kann ein Schritt S24 vorgesehen sein, in dem eine dritte Einmalkennung EK3 abhängig von der zweiten Einmalkennung EK2 ermittelt wird. Die dritte Einmalkennung EK3 wird dabei vorzugsweise durch einmaliges oder mehrmaliges Anwenden der vorgegebenen Rechenvorschrift ermittelt, falls die erste und die zweite Einmalkennung EK1, EK2 durch eine der Sendestationen aus der Kennungsliste ermittelt wurden. Ferner kann ein Schritt S25 vorgesehen sein, um den zweiten Nachrichtenprüfwert NP2 abhängig von der Nachricht N und der zweiten Einmalkennung EK2 zu ermitteln, falls die Nachricht N den ersten Nachrichtenprüfwert NP1 umfasst.

[0067] Ferner kann ein Schritt S26 vorgesehen sein zur Auswertung und Überprüfung der gegebenenfalls in der Nachricht N enthaltenen geographischen Gebietsinformation GEO_INF und/oder Anwendungsinformation ANW_INF. Dazu wird beispielsweise eine aktuelle geographische Position POS des Fahrzeugs ermittelt. Ferner wird das geographische Gebiet GEO abhängig von

der geographischen Gebietsinformations GEO_INF und gegebenenfalls der Anwendungsinformation ANW_INF ermittelt, für das die erste Einmalkennung EK1 Gültigkeit besitzt.

[0068] In einem Schritt S27 wird überprüft, ob die erste Einmalkennung EK1 mit der zweiten Einmalkennung EK2 übereinstimmt und/oder ob die dritte Einmalkennung EK3 mit der ersten Einmalkennung EK1 übereinstimmt und/oder ob der erste Nachrichtenprüfwert NP1 mit dem zweiten Nachrichtenprüfwert NP2 übereinstimmt und/oder ob die aktuelle geographische Position POS innerhalb des geographischen Gebiets GEO liegt, in der die erste Einmalkennung EK1 Gültigkeit besitzt. Ferner kann vorgesehen sein, den gegebenenfalls der ersten Einmalkennung EK1 und/oder der zweiten Einmalkennung EK2 beigefügten Kennungsprüfwert KP zu überprüfen.

[0069] Ist die jeweils relevante Bedingung in dem Schritt S27 erfüllt, dann wird die Nachricht N in einem Schritt S28 als gültig erkannt und in einem Schritt S29 gegebenenfalls wieder ausgsandt, zum Beispiel an andere Fahrzeuge oder Sendestationen. Das Programm wird in einem Schritt S30 beendet. Sind die Bedingungen in dem Schritt S27 jedoch nicht erfüllt, dann wird die Nachricht N in dem Schritt S31 als ungültig erkannt und das Programm in dem Schritt S30 beendet. Das Programm wird vorzugsweise für jede empfangene Nachricht N erneut ausgeführt.

[0070] Mittels der zeitlich und räumlich wechselnden Einmalkennungen EK kann die zeitliche Aktualität und die räumliche Relevanz von Nachrichten N auf einfache Weise festgestellt werden. Dadurch, dass die Einmalkennungen EK nicht vorhersagbar erzeugt werden, ist eine hohe Sicherheit und Zuverlässigkeit möglich. Dies gilt insbesondere, wenn die Einmalkennungen EK durch vertrauenswürdige Infrastruktureinheiten oder Sendestationen, zum Beispiel einer Verkehrsdateninfrastruktur, ausgestrahlt werden und jeweils durch einen Kennungsprüfwert KP geschützt sind. Unbefugte Manipulationen der Einmalkennungen EK oder Nachrichten N sind so einfach erkennbar. Durch die empfangenen Einmalkennungen EK kann insbesondere eine Fahrzeug-zu-Fahrzeug-Kommunikation geschützt werden, ohne dass dazu synchronisierte Uhren oder Positionsermittlungseinheiten in den Fahrzeugen, wie zum Beispiel GPS, erforderlich sind. Ferner ist es auf diese Weise nicht erforderlich, dass jeweils zwischen zwei Fahrzeugen oder zwischen einem Fahrzeug und einer Sendestation eine bidirektionale Kommunikationsverbindung aufgebaut werden muss, um Nachrichten N vor unbefugter Manipulation geschützt versenden und/oder empfangen zu können. Die Kommunikation kann somit spontan erfolgen durch einfaches Aussenden der jeweiligen Nachricht N ohne vorherige Kontaktaufnahme mit potentiellen Empfängern der Nachricht N.

Patentansprüche

1. Prüfverfahren zum Überprüfen einer Nachricht (N), die eine erste Einmalkennung (EK1) oder einen abhängig von der ersten Einmalkennung (EK1) ermittelten ersten Nachrichtenprüfwert (NP1) umfasst, bei dem

   - die Nachricht (N) per Funk empfangen wird,
   - eine per Funk ausgestrahlte zweite Einmalkennung (EK2) unabhängig von der Nachricht (N) empfangen wird und
   - die Nachricht (N) abhängig von der ersten Einmalkennung (EK1) und der zweiten Einmalkennung (EK2) auf ihre Gültigkeit überprüft wird und die Nachricht (N) als gültig erkannt wird, wenn die erste Einmalkennung (EK1) und die zweite Einmalkennung (EK2) übereinstimmen oder wenn der erste Nachrichtenprüfwert (NP1) mit einem zweiten Nachrichtenprüfwert (NP2) übereinstimmt, der abhängig von der zweiten Einmalkennung (EK2) ermittelt wird, oder wenn eine abhängig von der zweiten Einmalkennung (EK2) ermittelte dritte Einmalkennung (EK3) mit der ersten Einmalkennung (EK1) übereinstimmt, und die Nachricht (N) andernfalls als ungültig erkannt wird.

2. Prüfverfahren nach Anspruch 1, bei dem

   - eine geographische Gebietsinformation (GEO_INF) zu der ersten Einmalkennung (EK1) und/oder zu der zweiten Einmalkennung (EK2) ermittelt wird,
   - eine aktuelle geographische Position (POS) eines dieses Verfahren aktuell ausführenden Empfängers der Nachricht (N) ermittelt wird und
   - die Nachricht (N) abhängig von der geographischen Gebietsinformation (GEO_INF) und der ermittelten aktuellen geographischen Position (POS) auf ihre Gültigkeit überprüft wird und die Nachricht (N) als gültig erkannt wird, wenn die ermittelte aktuelle geographische Position (POS) innerhalb eines geographischen Gebiets (GEO) liegt, das abhängig von der geographischen Gebietsinformation (GEO_INF) vorgegeben wird, und die Nachricht (N) andernfalls als ungültig erkannt wird.

3. Prüfverfahren nach Anspruch 2, bei dem

   - eine Anwendungsinformation (ANW_INF) zu der ersten Einmalkennung (EK1) und/oder zu der zweiten Einmalkennung (EK2) ermittelt wird und
   - eine Größe des geographischen Gebiets (GEO) abhängig von der Anwendungsinformation (ANW_INF) vorgegeben wird.

4. Prüfverfahren nach einem der Ansprüche 2 oder 3, bei dem die geographische Gebietsinformation (GEO_INF) und/oder die Anwendungsinformation (ANW_INF) der ersten Einmalkennung (EK1) und/oder der zweiten Einmalkennung (EK2) beigefügt ist.

5. Prüfverfahren nach einem der Ansprüche 2 oder 3, bei dem die geographische Gebietsinformation (GEO_INF) und/oder die Anwendungsinformation (ANW_INF) von einem Server (SERV) abgerufen wird für die erste Einmalkennung (EK1) und/oder für die zweite Einmalkennung (EK2).

6. Prüfverfahren nach einem der vorstehenden Ansprüche, bei dem

- der ersten Einmalkennung (EK1) und/oder der zweiten Einmalkennung (EK2) ein jeweiliger Kennungsprüfwert (KP) beigefügt ist, der abhängig von der ersten Einmalkennung (EK1) beziehungsweise der zweiten Einmalkennung (EK2) ermittelt wurde,
- eine Gültigkeit der ersten Einmalkennung (EK1) beziehungsweise der zweiten Einmalkennung (EK2) abhängig von einem dem jeweiligen Empfänger der Nachricht (N) bekannten Schlüssel und abhängig von der ersten Einmalkennung (EK1) beziehungsweise der zweiten Einmalkennung (EK2) überprüft wird und
- die Nachricht (N) nur dann als gültig erkannt wird, wenn die Gültigkeit der ersten Einmalkennung (EK1) beziehungsweise der zweiten Einmalkennung (EK2) festgestellt wurde.

7. Prüfverfahren nach einem der vorstehenden Ansprüche, bei dem die dritte Einmalkennung (EK3) durch einmaliges oder mehrmaliges rekursives Anwenden einer vorgegebenen Rechenvorschrift abhängig von der zweiten Einmalkennung (EK2) ermittelt wird.

8. Prüfverfahren nach einem der vorstehenden Ansprüche, bei dem die als gültig erkannte Nachricht (N) per Funk ausgesandt wird.

9. Prüfvorrichtung zum Überprüfen einer Nachricht (N), die eine erste Einmalkennung (EK1) oder einen abhängig von der ersten Einmalkennung (EK1) ermittelten ersten Nachrichtenprüfwert (NP1) umfasst, die ausgebildet ist

- zum Empfangen der Nachricht (N) per Funk,
- zum Empfangen einer per Funk ausgestrahlten zweiten Einmalkennung (EK2) unabhängig von der Nachricht (N) und
- zum Überprüfen der Nachricht (N) abhängig von der ersten Einmalkennung (EK1) und der zweiten Einmalkennung (EK2) auf ihre Gültigkeit, wobei die Nachricht (N) als gültig erkannt wird, wenn die erste Einmalkennung (EK1) und die zweite Einmalkennung (EK2) übereinstimmen oder wenn der erste Nachrichtenprüfwert (NP1) mit einem zweiten Nachrichtenprüfwert (NP2) übereinstimmt, der abhängig von der zweiten Einmalkennung (EK2) ermittelt wird, oder wenn eine abhängig von der zweiten Einmalkennung (EK2) ermittelte dritte Einmalkennung (EK3) mit der ersten Einmalkennung (EK1) übereinstimmt, und die Nachricht (N) andernfalls als ungültig erkannt wird.

10. Sendeverfahren zum Aussenden einer Nachricht (N), bei dem

- eine per Funk ausgestrahlte Einmalkennung (EK) empfangen wird,
- der Nachricht (N) die empfangene Einmalkennung (EK) oder ein Nachrichtenprüfwert (NP), der abhängig von der empfangenen Einmalkennung (EK) ermittelt wird, hinzugefügt wird und
- die Nachricht (N) per Funk ausgesandt wird.

11. Sendevorrichtung zum Aussenden einer Nachricht (N), die ausgebildet ist

- zum Empfangen einer ausgestrahlten Einmalkennung (EK) per Funk,
- zum Hinzufügen der empfangenen Einmalkennung (EK) oder eines Nachrichtenprüfwerts (NP), der abhängig von der empfangenen Einmalkennung (EK) ermittelt wird, zu der Nachricht (N) und
- zum Aussenden der Nachricht (N) per Funk.

12. Sendeverfahren zum Aussenden von Einmalkennungen (EK) durch eine Sendestation, bei dem

- jeweils mindestens eine Einmalkennung (EK) in einem vorgegebenen Zeitintervall (ZI) ermittelt wird, wobei die jeweilige Einmalkennung (EK) individuell und eindeutig für die Sendestation und für das jeweilige Zeitintervall ermittelt wird, und
- die jeweils mindestens eine Einmalkennung (EK) per Funk ausgestrahlt wird.

13. Sendeverfahren nach Anspruch 12, bei dem die jeweilige Einmalkennung (EK) ermittelt wird durch Auswahl eines jeweils nächsten Listeneintrags einer Kennungsliste, deren Listeneinträge jeweils erzeugt werden durch rekursives Anwenden einer vorgegebenen Rechenvorschrift abhängig von einer vorgegebenen Anfangskennung.

14. Sendeverfahren nach Anspruch 12, bei dem die jeweilige Einmalkennung (EK) ermittelt wird als ein Zu-

fallswert oder Pseudozufallswert.

15. Sendeverfahren nach einem der Ansprüche 12 bis 14, bei dem die jeweils ermittelte Einmalkennung (EK) für eine vorgegebene Zeitdauer wiederholt ausgesandt wird, die länger ist als das vorgegebene Zeitintervall (ZI).

16. Sendeverfahren nach einem der Ansprüche 12 bis 15, bei dem mindestens eine Einmalkennung (EK) von einer benachbarten Sendestation empfangen und zusätzlich ausgesandt wird.

17. Sendeverfahren nach einem der Ansprüche 12 bis 16, bei dem Nachrichten (N) empfangen, überprüft und gegebenenfalls ausgesandt werden, wobei die jeweilige Nachricht (N) eine erste Einmalkennung (EK1) oder einen abhängig von der ersten Einmalkennung (EK1) ermittelten ersten Nachrichtenprüfwert (NP1) umfasst und das Überprüfen der jeweiligen Nachricht (N) abhängig von der ersten Einmalkennung (EK1) und mindestens einer der Einmalkennungen (EK) der Sendestation und/oder der benachbarten Sendestation durchgeführt wird und die jeweilige Nachricht (N) nur dann ausgesandt wird, wenn die erste Einmalkennung (EK1) und die mindestens eine der Einmalkennungen (EK) der Sendestation oder der benachbarten Sendestation übereinstimmen oder wenn der erste Nachrichtenprüfwert (NP1) mit einem zweiten Nachrichtenprüfwert (NP2) übereinstimmt, der abhängig von der mindestens einen der Einmalkennungen (EK) der Sendestation und/oder der benachbarten Sendestation ermittelt wird.

18. Sendeverfahren nach einem der Ansprüche 12 bis 17, bei dem der jeweiligen Einmalkennung (EK) eine geographische Gebietsinformation (GEO_INF) und/oder eine Anwendungsinformation (ANW_INF) und/oder eine Gültigkeitsdauer beigefügt wird.

19. Sendeverfahren nach einem der Ansprüche 12 bis 18, bei dem
der jeweiligen Einmalkennung (EK) ein jeweiliger Kennungsprüfwert (KP) beigefügt wird, der abhängig von der jeweiligen Einmalkennung (EK) ermittelt wird.

20. Sendestation, die eine Zeitmesseinheit (ZME) und eine Sendeeinheit (SE) aufweist und die ausgebildet ist

- zum Ermitteln jeweils mindestens einer Einmalkennung (EK) in einem vorgegebenen Zeitintervall (ZI), das mittels der Zeitmesseinheit (ZME) vorgegeben wird, wobei die jeweilige Einmalkennung (EK) individuell und eindeutig für die Sendestation und für das jeweilige Zeitintervall ermittelt wird, und
- zum Ausstrahlen der jeweils mindestens einen Einmalkennung (EK) mittels der Sendeeinheit (SE) per Funk.

21. System, das mindestens zwei Sendestationen nach Anspruch 20 und mindestens zwei Prüf- und/oder Sendevorrichtungen (SV, PV) nach Anspruch 9 beziehungsweise 11 umfasst.

FIG 1

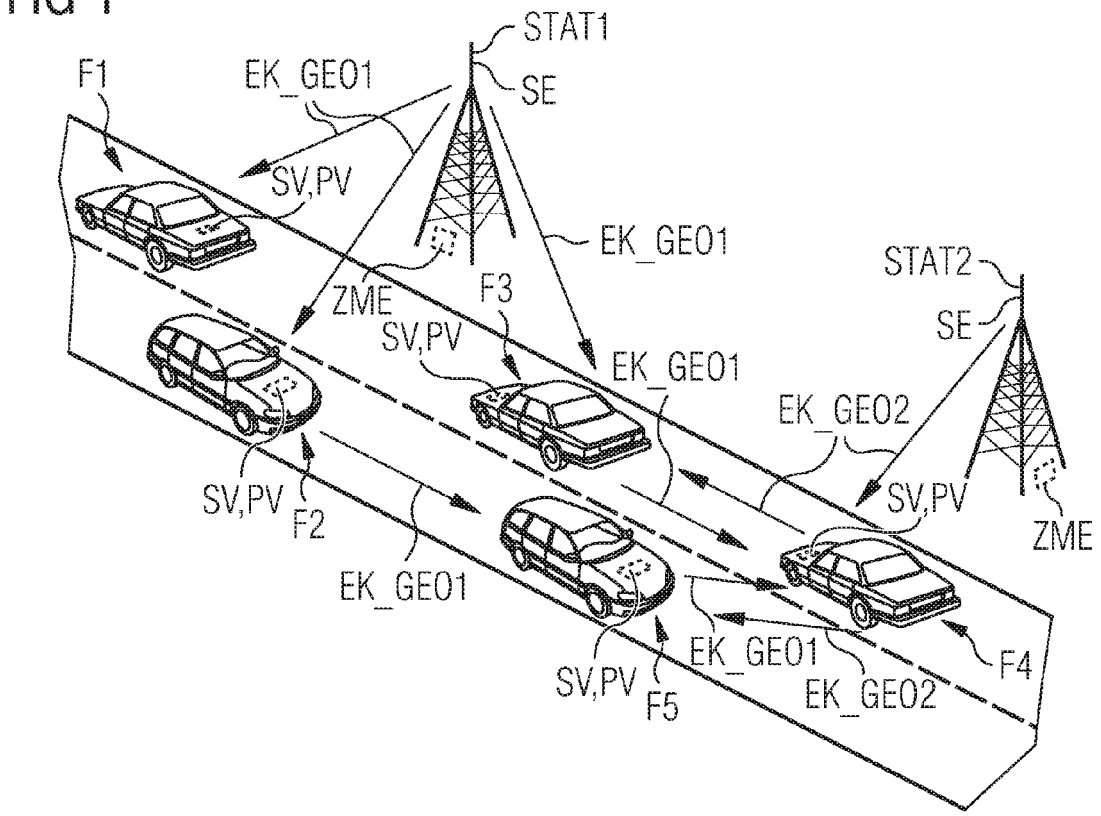

STAT1
SE
F1
EK_GEO1
SV,PV
EK_GEO1
ZME
F3
SV,PV
EK_GEO1
STAT2
SE
EK_GEO2
SV,PV
ZME
SV,PV
F2
EK_GEO1
SV,PV
F5
EK_GEO1
EK_GEO2
F4

FIG 2

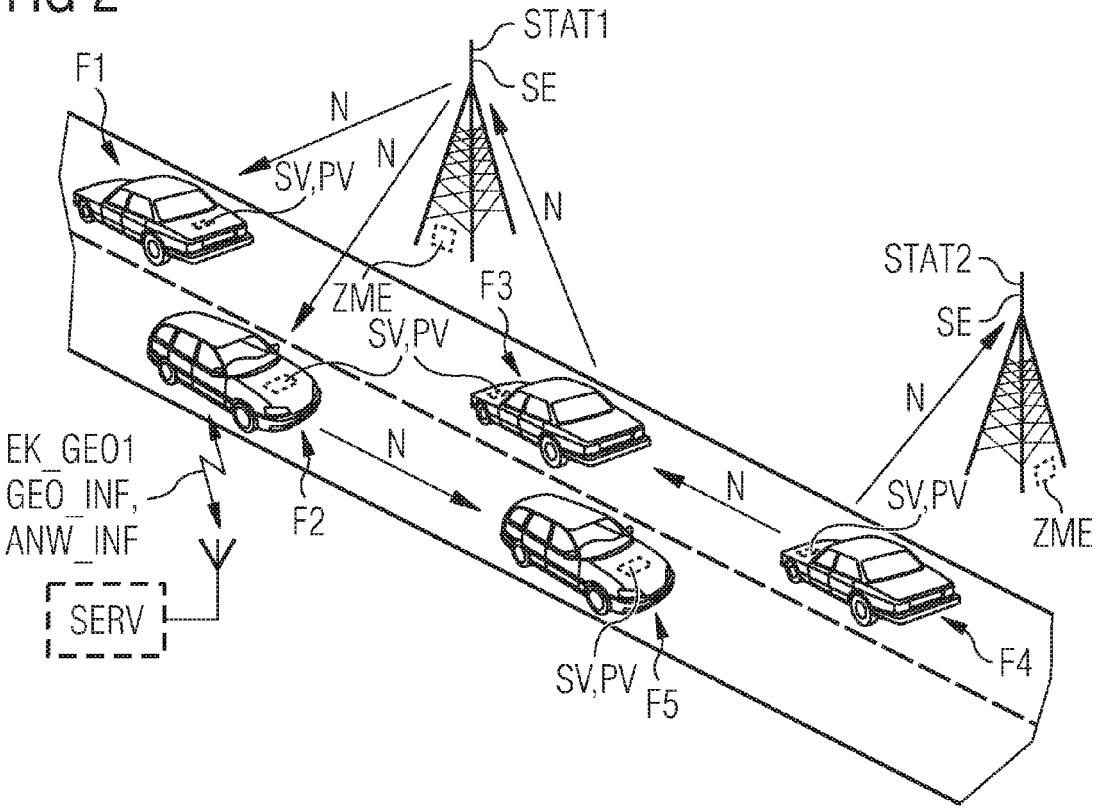

STAT1
SE
F1
N
SV,PV
N
N
ZME
F3
SV,PV
STAT2
SE
N
EK_GEO1
GEO_INF,
ANW_INF
SERV
F2
N
N
SV,PV
ZME
SV,PV
F5
F4

FIG 3

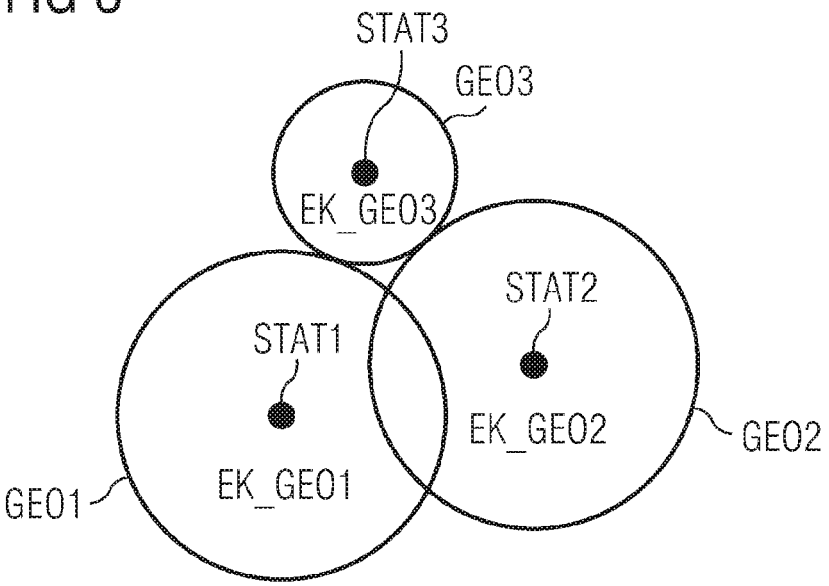

STAT3
GEO3
EK_GEO3
STAT2
STAT1
EK_GEO2
GEO2
EK_GEO1
GEO1

FIG 4

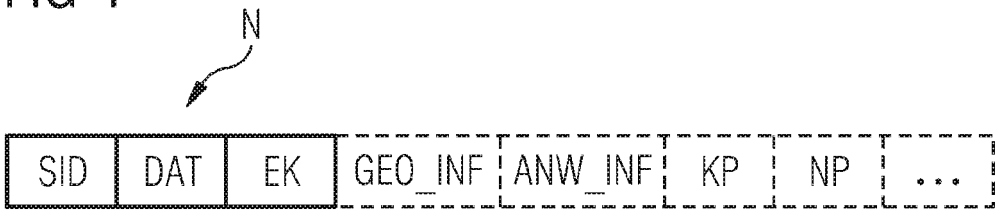

N
SID
DAT
EK
GEO_INF
ANW_INF
KP
NP
...

FIG 5

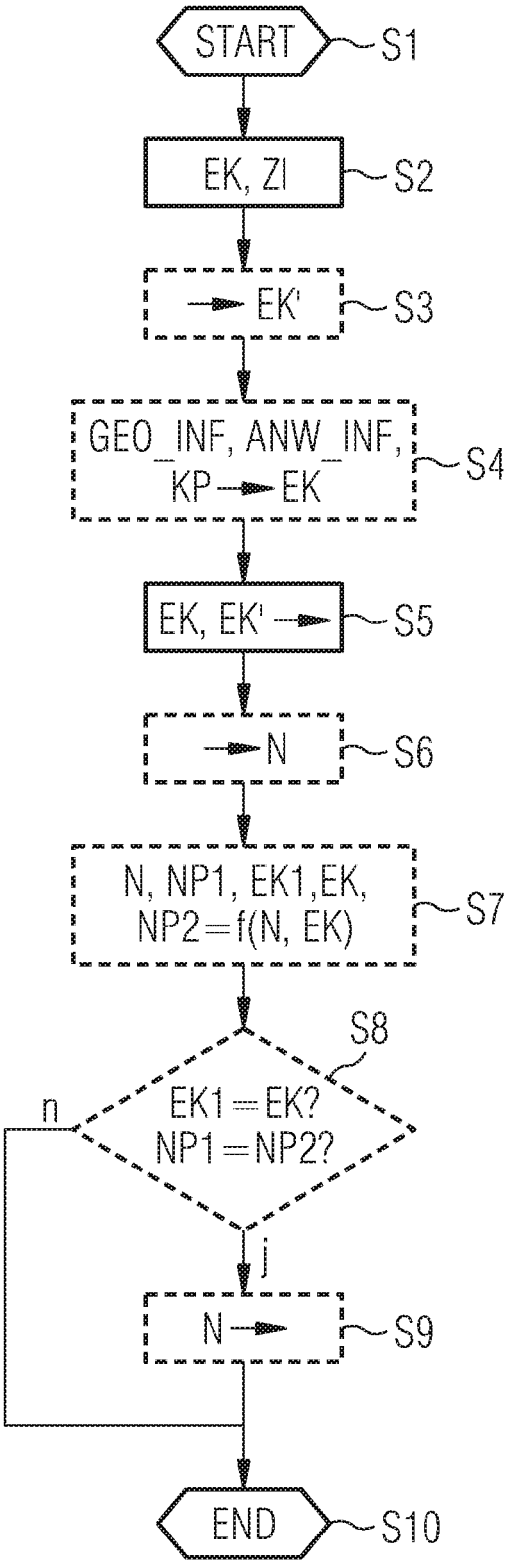

START
S1
EK, ZI
S2
EK'
S3
GEO_INF, ANW_INF,
KP → EK
S4
EK, EK'
S5
N
S6
N, NP1, EK1, EK,
NP2 = f(N, EK)
S7
S8
EK1 = EK?
NP1 = NP2?
n
j
N
S9
END
S10

FIG 6

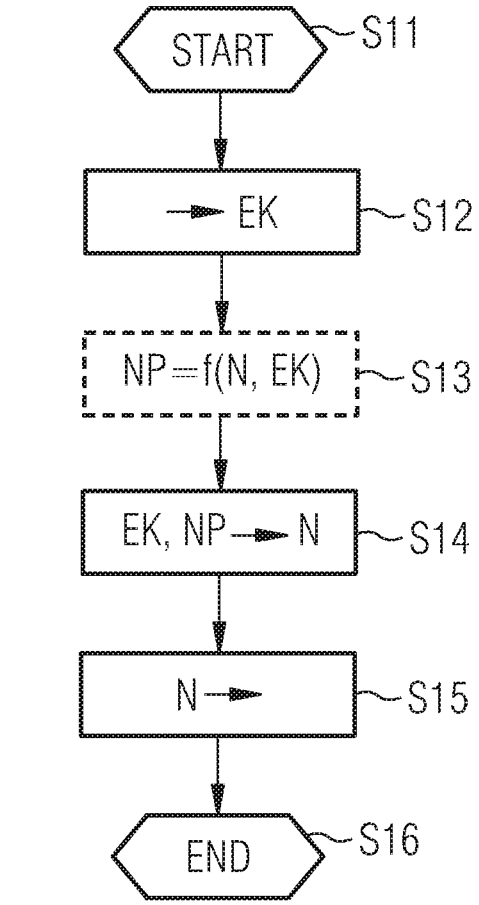
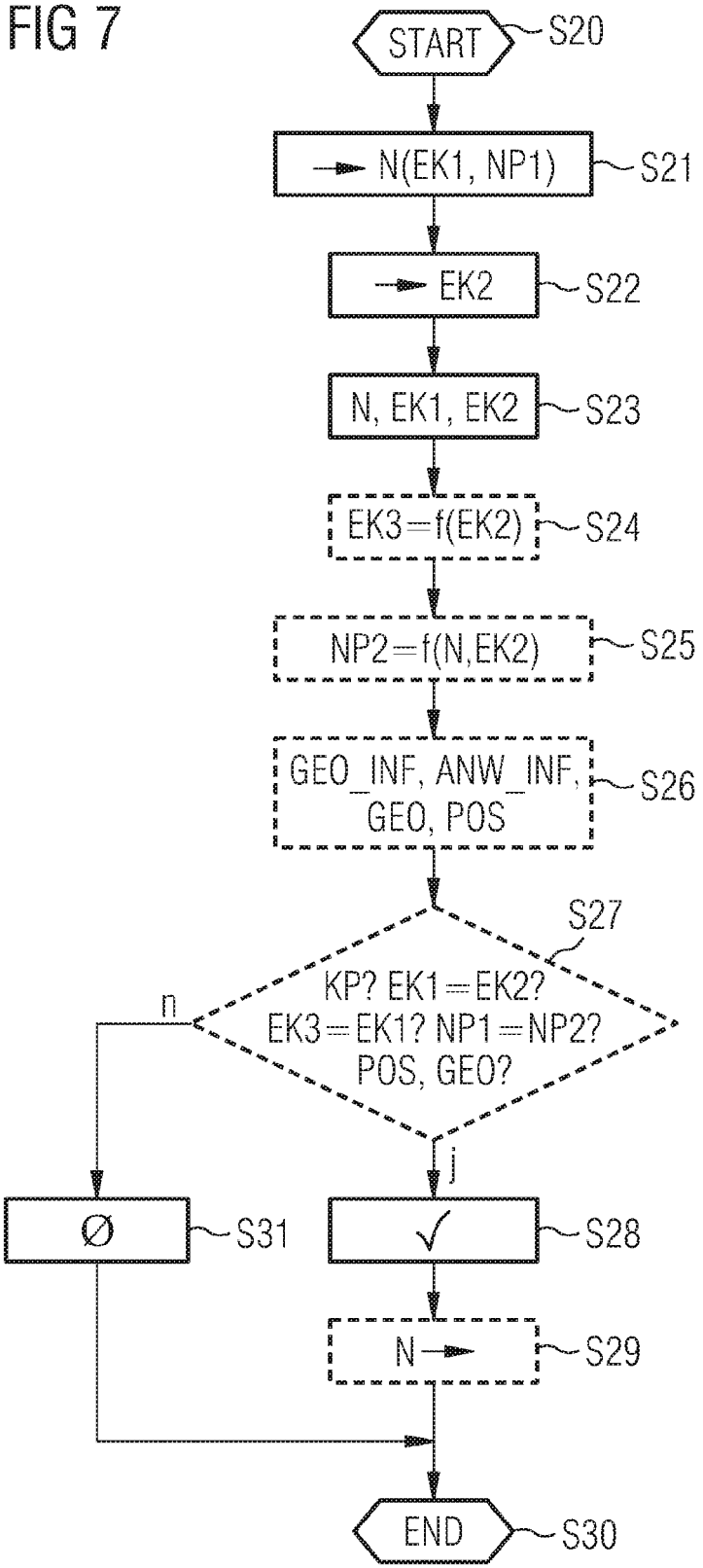


FIG 7


START
S20
N(EK1, NP1)
S21
EK2
S22
N, EK1, EK2
S23
EK3=f(EK2)
S24
NP2=f(N,EK2)
S25
GEO_INF, ANW_INF, GEO, POS
S26
S27
KP? EK1=EK2? EK3=EK1? NP1=NP2? POS, GEO?
n
j
Ø
S31
✓
S28
N
S29
END
S30