(19) Deutsches Patent- und Markenamt

(10) **DE 10 2023 202 190 A1** 2024.09.12

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2023 202 190.0**
(22) Anmeldetag: **10.03.2023**
(43) Offenlegungstag: **12.09.2024**

(51) Int Cl.: ***H04W 12/108*** (2021.01)
H04W 4/40 (2018.01)
G08G 1/0965 (2006.01)

(71) Anmelder:
Robert Bosch Gesellschaft mit beschränkter Haftung, 70469 Stuttgart, DE

(72) Erfinder:
Friedrich, Michael, 73104 Börtlingen, DE; Wienss, Andreas, 72800 Eningen, DE

(56) Ermittelter Stand der Technik:

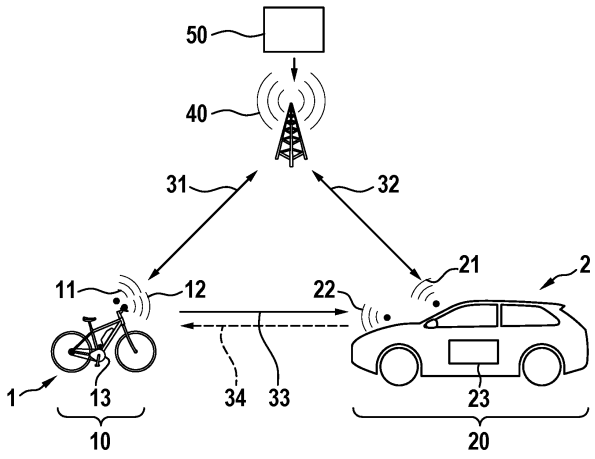
US	**2015 / 0 279 122**	**A1**
US	**2019 / 0 184 993**	**A1**
US	**2020 / 0 008 059**	**A1**
US	**2021 / 0 297 881**	**A1**
US	**2022 / 0 038 296**	**A1**

Rechercheantrag gemäß § 43 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Kommunikationseinheiten und zugehöriges Kommunikationssystem für eine Kommunikation zwischen Verkehrsteilnehmern**

(57) Zusammenfassung: Die vorliegende Erfindung betrifft eine erste Kommunikationsvorrichtung (10) für einen ersten Verkehrsteilnehmer (1), umfassend eine erste Sendeeinheit (11), welche dazu eingerichtet ist, Informationen über eine Funkverbindung erster Art zu senden, eine zweite Sendeeinheit (12), welche dazu eingerichtet ist, Informationen über eine Funkverbindung zweiter Art zu senden, und eine Steuereinheit (13) der ersten Kommunikationsvorrichtung (10), welche dazu eingerichtet ist, dem ersten Verkehrsteilnehmer (1) zugehörige kryptografische erste Informationen über die erste Sendeeinheit (11) zu senden, und dem ersten Verkehrsteilnehmer (1) zugehörige Zustandsinformationen zusammen mit kryptografischen zweiten Informationen über die zweite Sendeeinheit (12) zu senden, wobei die kryptografischen ersten Informationen dazu geeignet sind, die Zustandsinformationen mittels der kryptografischen zweiten Informationen zu verifizieren.



Beschreibung

Stand der Technik

[0001] Zwischen motorisierten Fahrzeugen wird es in Zukunft mehr und mehr Kommunikation geben, wobei diese Kommunikation sowohl über größere Distanz, z. B. über 4G, 5G, als auch über kurze Distanz, z. B. über den WiFi basierten ITS-G5-Standard oder den in 4G/5G ab Release 14 enthaltenen Sidelink, erfolgt. Ein Hauptziel dieser Kommunikation ist Unfallvermeidung durch erhöhte Wahrnehmungen, Warnungen bis hin zu koordinierten Manövern und automatisierte Eingriffe. Spätestens automatisiert fahrende Fahrzeuge werden solche Technologien benötigen, welche beispielsweise als Blickkontaktersatz eingesetzt werden können.

[0002] Dabei kann in Betracht gezogen werden, auch vulnerable Verkehrsteilnehmer, sogenannte VRUs (Vulnerable Road User), an dieser Kommunikation teilhaben zu lassen. Auf diese Weise können auch Unfälle zwischen motorisierten Fahrzeugen und VRUs, beispielsweise Fahrrädern oder Fußgängern, vermieden werden.

[0003] Dabei können und werden momentan die folgenden Ansätze verfolgt:

- Über einen 4G/5G-basierten Ansatz können Smartphones dazu eingerichtet sein, Position und Richtung des VRU an einen Server zu senden, welcher Kollisionswahrscheinlichkeiten berechnet oder an die in der Umgebung befindlichen Verkehrsteilnehmer weiterleitet. Im Bedarfsfall können Warnungen von dem Server zurückgeschickt werden.
- Fahrradcomputer können direkt mit motorisierten Verkehrsteilnehmern kommunizieren, wie dies beispielsweise bei ITS-G5 und PC5 der Fall ist.
- Bluetooth-Funkverbindungen können von VRUs bereitgestellt werden, wobei von dem VRU jedoch nur Informationen ausgesendet werden, wodurch jedoch keine Warnung des VRUs erfolgen kann.

Offenbarung der Erfindung

[0004] Die erfindungsgemäße erste Kommunikationsvorrichtung für einen ersten Verkehrsteilnehmer umfasst eine erste Sendeeinheit, welche dazu eingerichtet ist, Informationen über eine Funkverbindung erster Art zu senden, eine zweite Sendeeinheit, welche dazu eingerichtet ist, Informationen über eine Funkverbindung zweiter Art zu senden, und eine Steuereinheit der ersten Kommunikationsvorrichtung, welche dazu eingerichtet ist, dem ersten Verkehrsteilnehmer zugehörige kryptografische erste Informationen über die erste Sendeeinheit zu senden und dem ersten Verkehrsteilnehmer zugehörige Zustandsinformationen zusammen mit kryptografischen zweiten Informationen über die zweite Sendeeinheit zu senden, wobei die kryptografischen ersten Informationen dazu geeignet sind, die Zustandsinformationen mittels der kryptografischen zweiten Informationen zu verifizieren.

[0005] Die erfindungsgemäße zweite Kommunikationsvorrichtung für einen zweiten Verkehrsteilnehmer umfasst eine erste Empfangseinheit, welche dazu eingerichtet ist, Informationen über eine Funkverbindung erster Art zu empfangen, eine zweite Empfangseinheit, welche dazu eingerichtet ist, Informationen über eine Funkverbindung zweiter Art zu empfangen, und eine Steuereinheit, welche dazu eingerichtet ist, einem ersten Verkehrsteilnehmer zugehörige kryptografische erste Informationen über die erste Empfangseinheit zu empfangen, dem ersten Verkehrsteilnehmer zugehörige Zustandsinformationen zusammen mit kryptografischen zweiten Informationen über die zweite Empfangseinheit zu empfangen und die Zustandsinformationen basierend auf den kryptografischen ersten Informationen mittels der kryptografischen zweiten Informationen zu verifizieren.

[0006] Das erfindungsgemäße Verfahren für eine Kommunikation zwischen einem ersten Verkehrsteilnehmer und einem zweiten Verkehrsteilnehmer umfasst ein Übertragen von dem ersten Verkehrsteilnehmer zugehörigen kryptografischen ersten Informationen von dem ersten Verkehrsteilnehmer an den zweiten Verkehrsteilnehmer mittels einer Funkverbindung erster Art, ein Übertragen von dem ersten Verkehrsteilnehmer zugehörigen Zustandsinformationen zusammen mit kryptografischen zweiten Informationen von dem ersten Verkehrsteilnehmer an den zweiten Verkehrsteilnehmer über eine Funkverbindung zweiter Art, wobei die kryptografischen ersten Informationen dazu geeignet sind, die Zustandsinformationen mittels der kryptografischen zweiten Informationen zu verifizieren, und ein Verifizieren der Zustandsinformationen basierend auf den kryptografischen ersten Informationen mittels der kryptografischen zweiten Informationen durch den zweiten Verkehrsteilnehmer.

[0007] Die Zustandsinformationen sind Informationen, welche einen Zustand oder Eigenschaft des ersten Verkehrsteilnehmers beschreiben. Bevorzugt sind die Zustandsinformationen solche Informationen, die im Rahmen einer V2X-Kommunikation ausgesendet werden. Die Zustandsinformationen sind insbesondere Positions- und/oder Bewegungsinformationen des ersten Verkehrsteilnehmers. Positionsinformationen sind dabei jegliche Informationen, welche eine Position des ersten Verkehrsteilnehmers beschreiben, wobei die Position als absolute oder relative Position beschrieben sein kann. Bewegungs-

informationen sind dabei jegliche Informationen, welche eine Bewegung des ersten Verkehrsteilnehmers beschreiben. Die Bewegung des ersten Verkehrsteilnehmers kann dabei beispielsweise durch eine Beschleunigung, Geschwindigkeit oder Trajektorie des Verkehrsteilnehmers beschrieben werden.

[0008] Die erste Kommunikationsvorrichtung umfasst die erste Sendeeinheit, welche dazu eingerichtet ist, Informationen über die Funkverbindung erster Art zu senden. Die zweite Kommunikationsvorrichtung umfasst die erste Empfangseinheit, welche dazu eingerichtet ist, Informationen über die Funkverbindung erster Art zu empfangen. Die Funkverbindung erster Art basiert auf einem anderen Kommunikationsstandard als die Funkverbindung zweiter Art. Die Funkverbindung erster Art ist eine direkte oder indirekte Funkverbindung zwischen der ersten Sendeeinheit der ersten Kommunikationsvorrichtung und der ersten Empfangseinheit der zweiten Kommunikationsvorrichtung. Eine indirekte Funkverbindung ist dabei eine Funkverbindung, bei der die Kommunikation über eine zwischenliegende Einheit weitergeleitet wird. Die Funkverbindung erster Art ist bevorzugt eine 4G, eine 5G eine WiFi oder eine LoRaWaN Kommunikationsverbindung. Dies umfasst auch die in 4G/5G ab Release 14 enthaltene Sidelink Kommunikationsverbindung.

[0009] Die erste Kommunikationsvorrichtung umfasst die zweite Sendeeinheit, welche dazu eingerichtet ist, Informationen über die Funkverbindung zweiter Art zu senden. Die zweite Kommunikationsvorrichtung umfasst die zweite Empfangseinheit, welche dazu eingerichtet ist, Informationen über die Funkverbindung zweiter Art zu empfangen. Die Funkverbindung zweiter Art ist eine direkte Funkverbindung. Die Funkverbindung zweiter Art ist insbesondere eine von der ersten Kommunikationsvorrichtung ausgehende Broadcastkommunikation. Die Funkverbindung zweiter Art ist insbesondere eine Bluetooth, UWB, ITS-G5 oder PC5 Kommunikationsverbindung.

[0010] Die Funkverbindung zweiter Art und die dafür verwendete erste Sendeeinheit der ersten Kommunikationsvorrichtung und erste Empfangseinheit der zweiten Kommunikationsvorrichtung ist bevorzugt für eine Kommunikation über größere Distanzen vorgesehen während die zweite Sendeeinheit der ersten Kommunikationsvorrichtung und die zweite Empfangseinheit der zweiten Kommunikationsvorrichtung für eine Kommunikation im Nahfeld der ersten Kommunikationsvorrichtung vorgesehen ist.

[0011] Die erste Kommunikationsvorrichtung als auch die zweite Kommunikationsvorrichtung umfasst jeweils eine Steuereinheit, welche beispielsweise eine Recheneinheit ist, durch welche die Aktionen der jeweiligen Kommunikationsvorrichtung koordiniert werden. Die kryptografischen ersten Informationen sind dazu geeignet, die über die Funkverbindung zweiter Art bereitgestellten Zustandsinformationen des ersten des Verkehrsteilnehmers sicher zuzuordnen oder optional ein Abhören der Daten zu vermeiden. Die kryptografischen ersten Informationen umfassen somit insbesondere auch Informationen, welche für ein Signieren von Daten geeignet sind, um deren Zugehörigkeit zu der ersten Kommunikationsvorrichtung des ersten Verkehrsteilnehmers zu bestätigen. Die dem ersten Verkehrsteilnehmer zugehörigen ersten kryptografischen Informationen dienen zum Etablieren eines gesicherten Datenaustauschs mit der zweiten Kommunikationsvorrichtung des zweiten Verkehrsteilnehmers. Durch die kryptografischen Informationen kann der Datenaustausch somit derart gesichert werden, dass möglichst keine anderen Einheiten Informationen im Namen des ersten Verkehrsteilnehmers aussenden können.

[0012] Die Zustandsinformationen sind dabei von dem ersten Verkehrsteilnehmer derart signiert und/oder verschlüsselt oder in ähnlicher Weise gesichert worden, dass diese mittels der kryptografischen ersten Informationen gelesen oder zumindest dem ersten Verkehrsteilnehmer sicher zugeordnet werden können. In diesem Fall ist der Datenaustausch ein gesicherter Datenaustausch.

[0013] Die Unteransprüche zeigen bevorzugte Weiterbildungen der Erfindung.

[0014] Bevorzugt ist die erste Sendeeinheit der ersten Kommunikationsvorrichtung dazu eingerichtet, Informationen über ein Funknetzwerk an einen Kommunikationsserver zu senden und die Steuereinheit der ersten Kommunikationsvorrichtung ist dazu eingerichtet, die kryptografischen ersten Informationen an den Kommunikationsserver zu senden. Weiter bevorzugt ist die zweite Sendeeinheit dazu eingerichtet, die Zustandsinformationen zusammen mit den kryptografischen zweiten Informationen über eine direkte Funkverbindung an den zweiten Verkehrsteilnehmer zu senden. Ebenso vorteilhaft ist es, wenn die erste Empfangseinheit der zweiten Kommunikationsvorrichtung dazu eingerichtet ist, Informationen über ein Funknetzwerk von einem Kommunikationsserver zu empfangen und die Steuereinheit der zweiten Kommunikationsvorrichtung dazu eingerichtet ist, die kryptografischen ersten Informationen von dem Kommunikationsserver zu empfangen. Der Kommunikationsserver ist bevorzugt ein Applikationsserver oder ein GeoServer. Der Kommunikationsserver ist bevorzugt dazu eingerichtet, die Zustandsinformationen und/oder die kryptografischen zweiten Informationen teilweise oder vollständig für eine Verarbeitung oder Bewertung an einen weiteren Server weiterzuleiten. Weiter bevorzugt ist die zweite Empfangseinheit dazu eingerich-

tet, die Zustandsinformationen zusammen mit den kryptografischen zweiten Informationen über eine direkte Funkverbindung von dem ersten Verkehrsteilnehmer zu empfangen. Die Kommunikationsvorrichtungen sind somit dazu eingerichtet, Informationen über ein Funknetzwerk zu übertragen und über einen Kommunikationsserver auszutauschen. Das Funknetzwerk ist dabei insbesondere ein Mobilfunknetzwerk. Der Kommunikationsserver ist insbesondere ein Internetserver, welcher über eine von dem Funknetzwerk bereitgestellte Internetverbindung kontaktiert werden kann, um Daten auf diesen hochzuladen oder von diesem herunterzuladen. Insbesondere werden von dem Applikationsserver Nachrichten an die zweite Kommunikationsvorrichtung gesendet, um die kryptografische erste Information zu übertragen.

[0015] Bevorzugt ist die ersten Kommunikationsvorrichtung eine mobile Einheit, insbesondere ein Fahrradcomputer oder ein Smartphone. Die mobile Einheit ist eine Einheit, welche von einem Anwender mit sich geführt werden kann, auch wenn dieser sich nicht in einem Kraftfahrzeugt bewegt. In diesem Falle ist der Anwender als vulnerabler Verkehrsteilnehmer anzusehen. Der erste Verkehrsteilnehmer ist bevorzugt ein Fußgänger oder ein Fahrradfahrer. Weiter bevorzugt ist der zweite Verkehrsteilnehmer ein Kraftfahrzeug. Die zweite Kommunikationsvorrichtung des zweiten Verkehrsteilnehmers ist dabei insbesondere eine Kommunikationsvorrichtung, welche auch im Rahmen einer V2X-Kommunikation zum Aussenden von Informationen, insbesondere von Positions- und/oder Bewegungsinformationen genutzt wird.

[0016] Bevorzugt umfassen die dem ersten Verkehrsteilnehmer zugehörigen kryptografischen ersten Informationen ein digitales Zertifikat und die dem zweiten Verkehrsteilnehmer gesendeten kryptografischen zweiten Informationen umfassen einen Hashwert, welcher basierend dem digitalen Zertifikat generiert wurde. Auf diese Weise kann den Verkehrsteilnehmern bevorzugt über einen Zertifikatsserver ein gesicherter Datenaustausch ermöglicht werden, wobei es der zweiten Kommunikationsvorrichtung ermöglicht wird, sicherzustellen, dass die empfangenen Zustandsinformationen tatsächlich von dem ersten Verkehrsteilnehmer ausgesendet wurden und nicht von einer anderen Einheit ausgesendet wurden. Die Steuereinheit der ersten Kommunikationsvorrichtung ist dabei bevorzugt dazu eingerichtet, die Zustandsinformationen basierend auf den kryptografischen ersten Informationen zu signieren, indem diese basierend auf den Zustandsinformationen die kryptografischen zweiten Informationen berechnet. Die Steuereinheit der zweiten Kommunikationsvorrichtung ist dabei bevorzugt dazu eingerichtet, um mittels der kryptografischen ersten Informationen zu überprüfen, ob die Zustandsinformationen den kryptografischen zweiten Informationen zugehörig sind. Mit anderen Worten bedeutet dies, dass die Zustandsinformationen von der ersten Kommunikationsvorrichtung signiert werden und die Signatur von der zweiten Kommunikationsvorrichtung geprüft wird.

[0017] Bevorzugt ist die erste Sendeeinheit der ersten Kommunikationsvorrichtung für eine Übertragung über eine größere Reichweite vorgesehen als die zweite Sendeeinheit der ersten Kommunikationsvorrichtung. Bevorzugt ist die erste Empfangseinheit der zweiten Kommunikationsvorrichtung für eine Übertragung über eine größere Reichweite vorgesehen als die zweite Empfangseinheit der zweiten Kommunikationsvorrichtung. Das bedeutet, dass die Funkverbindung der ersten Art eine größere Reichweite überbrücken kann, als die Funkverbindung der zweiten Art. Somit können die kryptografischen ersten Informationen bereits mittels der Funkverbindung der ersten Art bereits übersendet werden, bevor überhaupt eine Kommunikation mittels der Funkverbindung der zweiten Art erfolgen kann. Die kryptografischen ersten Informationen sind damit bereits verfügbar, wenn diese für das Verifizieren der Zustandsinformationen benötigt werden.

[0018] Bevorzugt ist die erste Sendeeinheit der ersten Kommunikationsvorrichtung dazu eingerichtet, größere Datenpakete zu übertragen als die zweite Sendeeinheit der ersten Kommunikationsvorrichtung. Ebenso bevorzugt ist die erste Empfangseinheit der zweiten Kommunikationsvorrichtung dazu eingerichtet, größere Datenpakete zu übertragen als die zweite Empfangseinheit der zweiten Kommunikationsvorrichtung. Es ist somit bevorzugt die Funkverbindung der ersten Art dazu geeignet, größere Datenpakete und, bevorzugt über längere Reichweiten, zu übertragen als die Funkverbindung der zweiten Art. Bevorzugt ist die Funkverbindung der zweiten Art dazu geeignet, Datenpakete mit einer niedrigeren Latenz zu übertragen als die Funkverbindung der ersten Art. Es können dabei bevorzugt über die erste Sendeeinheit der ersten Kommunikationsvorrichtung größere Datenpakete übertragen werden, jedoch nicht so oft, wie die vergleichsweise kleineren Datenpakete durch die zweite Sendeeinheit der ersten Kommunikationsvorrichtung übertragen werden. Damit kann dann die Paketgröße der zweiten Funkverbindung, durch Verwendung von Hashes statt der vollen Zertifikate, deutlich verringert bzw. überhaupt erst ermöglicht werden. So können beispielsweise bei einer Bluetooth-Low-Energy, BLE, Funkverbindung mit extended advertising maximal ca. 255 Bytes in einem Datenpaket übertragen werden.

[0019] Bevorzugt ist die Steuereinheit der zweiten Kommunikationsvorrichtung dazu eingerichtet, die über die zweite Empfangseinheit von dem ersten

Verkehrsteilnehmer empfangene Zustandsinformationen abhängig davon, ob die Zustandsinformationen mittels der kryptografischen zweiten Informationen erfolgreich verifiziert werden können, für unterschiedliche Unterstützungsfunktionen zu nutzen. Es ist somit vorteilhaft, wenn die Zustandsinformationen des ersten Verkehrsteilnehmers auch dann von der zweiten Kommunikationsvorrichtung empfangen werden, wenn diese nicht sicher dem ersten Verkehrsteilnehmer zugeordnet werden können, da die notwendigen kryptografischen ersten Informationen nicht vorliegen. Dies kann insbesondere dann der Fall sein, wenn diese von dem ersten Verkehrsteilnehmer nicht an den Kommunikationsserver übertragen wurden, diese der zweiten Kommunikationsvorrichtung von dem Kommunikationsserver nicht bereitgestellt wurden oder eine Funkkommunikation der ersten Art nicht möglich ist. Es wird damit der zweiten Kommunikationsvorrichtung ermöglicht selbst zu entscheiden, wie empfangene Zustandsinformationen genutzt werden. So können die empfangenen Zustandsinformationenbeispielsweise entweder ignoriert werden oder nur für nicht sicherheitskritische Anwendungen herangezogen werden, wenn die Verifizierung nicht möglich ist.

[0020] Es ist also vorteilhaft, wenn die Steuereinheit der zweiten Kommunikationsvorrichtung dazu eingerichtet ist, die über die zweite Empfangseinheit von dem ersten Verkehrsteilnehmer empfangenen Zustandsinformationen abhängig davon für unterschiedliche Unterstützungsfunktionen zu nutzen, ob diese über einen gesicherten Datenaustausch oder über einen nicht gesicherten Datenaustausch empfangen wurden. Unterstützungsfunktionen sind dabei Funktionen, welche einem Anwender durch die zweite Kommunikationsvorrichtung bereitgestellt werden. So wird einem Anwender durch die zweite Kommunikationsvorrichtung beispielsweise eine Kollisionswarnungsfunktion bereitgestellt, durch welche ein Anwender der zweiten Kommunikationsvorrichtung bezüglich möglicher Kollisionen mit dem Verkehrsteilnehmer hingewiesen wird. Ob beispielsweise empfangene Positions- und/oder Bewegungsinformationen für eine solche Warnmeldung einer Kollisionswarnungsfunktion genutzt werden, kann von der zweiten Kommunikationsvorrichtung entschieden werden.

[0021] Auch ist ein Informationssystem vorteilhaft, welches die erste Kommunikationsvorrichtung und/oder die zweite Kommunikationsvorrichtung umfasst und ferner den Kommunikationsserver umfasst. Dabei ist der Kommunikationsserver bevorzugt dazu eingerichtet, die dem ersten Verkehrsteilnehmer zugehörigen kryptografischen ersten Informationen in Reaktion darauf an die zweite Kommunikationsvorrichtung zu übertragen, dass eine vordefinierte erste Bedingung erfüllt ist, wobei die vordefinierte erste Bedingung insbesondere dann erfüllt ist, wenn dem Kommunikationsserver eine Information vorliegt, die auf einen zu erwartenden Datenaustausch zwischen der erste Kommunikationsvorrichtung und dem zweiten Verkehrsteilnehmer über die Funkverbindung zweiter Art schließen lässt. Es ist somit nicht notwendig, dass von dem Kommunikationsserver zu jedem Zeitpunkt alle verfügbaren kryptografischen ersten Informationen unterschiedlicher Verkehrsteilnehmer an die zweite Kommunikationsvorrichtung übertragen werden. Erst wenn davon ausgegangen werden kann, dass die zweite Kommunikationsvorrichtung mit dem ersten Verkehrsteilnehmer in einen Datenaustausch eintreten will, werden die kryptografischen ersten Informationen von dem Kommunikationsserver an die zweite Kommunikationsvorrichtung übertragen. Dabei ist es vorteilhaft, wenn beispielsweise kontinuierlich Positions- und/oder Bewegungsinformationen von der zweiten Kommunikationsvorrichtung und der ersten Kommunikationsvorrichtung an den Kommunikationsserver übertragen werden. Die kryptografischen ersten Informationen des ersten Verkehrsteilnehmers werden an die zweite Kommunikationsvorrichtung dann übertragen, wenn eine Annäherung zwischen der ersten Kommunikationsvorrichtung und der zweiten Kommunikationsvorrichtung erfolgt.

[0022] Bevorzugt ist der Kommunikationsserver dazu eingerichtet, das Übertragen der dem ersten Verkehrsteilnehmer zugehörigen kryptografischen ersten Informationen an den zweiten Verkehrsteilnehmer in Reaktion auf ein Vorliegen einer vordefinierten zweiten Bedingung zu unterbinden, wobei die vordefinierte zweite Bedingung insbesondere dann erfüllt ist, wenn dem Kommunikationsserver eine Information vorliegt, die auf eine eingeschränkte Vertrauenswürdigkeit des ersten Verkehrsteilnehmers schließen lässt. So wird durch den Kommunikationsserver beispielsweise ein ungewöhnliches Verhalten des Verkehrsteilnehmers detektiert. Auf diese Weise kann erkannt werden, ob durch den Verkehrsteilnehmer tatsächlich vertrauenswürdige Informationen bereitgestellt werden, oder ob möglicherweise eine Täuschung anderer Verkehrsteilnehmer erfolgen soll. Eine Vertrauenswürdigkeit ist dabei jedoch nicht auf Eigenschaften der Kommunikation beschränkt, sondern kann insbesondere basierend auf den Bereitgestellten Zustandsinformationen bewertet werden, wenn diese dem Kommunikationsserver übermittelt werden. In dem Falle einer als gering bewerteten Vertrauenswürdigkeit werden die kryptografischen ersten Informationen von dem Kommunikationsserver nicht der zweiten Kommunikationsvorrichtung bereitgestellt, wobei es jedoch in der Entscheidung der zweiten Kommunikationsvorrichtung liegt, ob die empfangenen Zustandsinformationen dennoch für bestimmte Unterstützungsfunktionen benutzt werden.

Kurze Beschreibung der Zeichnungen

[0023] Nachfolgend werden Ausführungsbeispiele der Erfindung unter Bezugnahme auf die begleitende Zeichnung im Detail beschrieben. In der Zeichnung ist:

Fig. 1 eine schematische Darstellung eines Kommunikationssystems, welches erfindungsgemäße Kommunikationsvorrichtungen umfasst,

Fig. 2 ein Ablaufdiagramm eines erfindungsgemäßen Verfahrens für eine Kommunikation zwischen zwei Kommunikationsvorrichtungen, und

Fig. 3 eine schematische Darstellung eines weiteren Kommunikationssystems, welches erfindungsgemäße Kommunikationsvorrichtungen umfasst.

Ausführungsformen der Erfindung

[0024] **Fig.** 1 zeigt ein erfindungsgemäßes Kommunikationssystem. Dieses umfasst eine erfindungsgemäße erste Kommunikationsvorrichtung 10, eine erfindungsgemäße zweite Kommunikationsvorrichtung 20, und einen Kommunikationsserver, welcher hier beispielhaft ein Applikationsserver 50 ist.

[0025] Die erste Kommunikationsvorrichtung 10 ist einem ersten Verkehrsteilnehmer 1 zugehörig und ist dazu beispielsweise ein Fahrradcomputer eines Fahrrades. Alternativ ist die erste Kommunikationsvorrichtung 10 ein Smartphone, welches beispielsweise an einem Fahrrad angeordnet ist oder von einem Fußgänger mit sich geführt wird. Die erste Kommunikationsvorrichtung 10 umfasst eine erste Sendeeinheit 11, welche dazu eingerichtet ist, Informationen über ein Funknetzwerk 40 an den Applikationsserver 50 zu übertragen. Optional umfasst die erste Kommunikationsvorrichtung 10 eine der ersten Sendeeinheit 11 der ersten Kommunikationsvorrichtung 10 zugehörige Empfangseinheit, um Informationen von dem Applikationsserver 50 über das Funknetzwerk 40 zu empfangen. Das Funknetzwerk 40 ist dabei ein Mobilfunknetzwerk.

[0026] Die zweite Kommunikationsvorrichtung 20 ist einem zweiten Verkehrsteilnehmer 2 zugehörig und ist dazu beispielsweise eine V2X-Einheit eines Kraftfahrzeuges. Die zweite Kommunikationsvorrichtung 20 umfasst eine erste Empfangseinheit 21, welche dazu eingerichtet ist, Informationen über das Funknetzwerk 40 von dem Applikationsserver 50 zu empfangen. Optional umfasst die zweite Kommunikationsvorrichtung 20 eine der ersten Empfangseinheit 21 der zweiten Kommunikationsvorrichtung 20 zugehörige Empfangseinheit, um Informationen von dem Applikationsserver 50 über das Funknetzwerk 40 zu empfangen. Ferner umfasst die erste Kommunikationsvorrichtung 10 eine zweite Sendeeinheit 12, welche dazu eingerichtet ist, Informationen über eine direkte Funkverbindung an eine zweite Empfangseinheit 22 der zweiten Kommunikationsvorrichtung 20 zu senden. Die zweite Sendeeinheit 12 der ersten Kommunikationsvorrichtung 10 ermöglicht eine direkte Funkverbindung zu der zweiten Empfangseinheit 22 der zweiten Kommunikationsvorrichtung 20. Das bedeutet, dass von der ersten Kommunikationsvorrichtung 10 des ersten Verkehrsteilnehmers 1 direkt und ohne eine zwischengeordnete Vorrichtung Informationen an den zweiten Verkehrsteilnehmer 20 übertragen werden können. Optional umfasst die erste Kommunikationsvorrichtung 10 auch eine zweite Empfangseinheit, welche der zweiten Sendeeinheit 12 zugeordnet ist und es ermöglicht über die direkte Funkverbindung Informationen von der zweiten Kommunikationsvorrichtung 20 zu empfangen. Der erste Verkehrsteilnehmer 1 und der zweite Verkehrsteilnehmer 2 sind zusammen mit der jeweils darin angeordneten Kommunikationsvorrichtung optional ein Teil des Kommunikationssystems.

[0027] Es wird somit über die erste Sendeeinheit 11 der ersten Kommunikationsvorrichtung 10 eine Kommunikation über größere Distanzen zu dem Applikationsserver 50 ermöglicht. Durch die zweite Sendeeinheit 12 der ersten Kommunikationsvorrichtung 10 bzw. durch die zweite Empfangseinheit 22 der zweiten Kommunikationsvorrichtung 20 wird eine Nahbereichskommunikation ermöglicht. Die Kommunikation über das Funknetzwerk 40 ist dabei eine Funkverbindung erster Art und die direkte Funkverbindung ist eine Funkverbindung zweiter Art. Dabei ist die Funkverbindung erster Art beispielsweise eine auf dem 4G oder 5G Standard basierende Kommunikationsverbindung. Die Funkverbindung zweiter Art ist beispielsweise eine auf einem V2X Standard basierende Kommunikationsverbindung, eine Bluetooth Verbindung oder eine UWB Verbindung. Die Funkverbindung zweiter Art weist bevorzugt eine geringere Latent auf als die Funkverbindung erster Art.

[0028] Durch den ersten Verkehrsteilnehmer 1 werden dem ersten Verkehrsteilnehmer 1 zugehörige erste kryptografische Informationen an den Applikationsserver 50 übertragen. Dies erfolgt über das Funknetzwerk 40. Ferner werden von der ersten Kommunikationsvorrichtung 10 mittels der zweiten Sendeeinheit 12 der ersten Kommunikationsvorrichtung 10 Zustandsinformationen des ersten Verkehrsteilnehmers 1 an die zweite Empfangseinheit 22 der zweiten Kommunikationsvorrichtung 20 übertragen. Die Zustandsinformationen sind beispielsweise Positionsinformationen des ersten Verkehrsteilnehmers 1. Ferner werden von der ersten Kommunikationsvorrichtung 10 mittels der zweiten Sendeeinheit 12 der ersten Kommunikationsvorrichtung 10 kryptografische zweite Informationen des ersten Verkehrsteil-

nehmers 1 an die zweite Empfangseinheit 22 der zweiten Kommunikationsvorrichtung 20 übertragen. Die kryptografischen ersten Informationen sind dazu geeignet, die Zustandsinformationen mittels der kryptografischen zweiten Informationen zu verifizieren. So sind die kryptografischen zweiten Informationen beispielsweise ein Hashwert oder eine Signatur der Zustandsinformationen, die basierend auf einem Zertifikat berechnet wurden, welches durch die ersten kryptografischen Informationen gegeben ist. Die kryptografischen ersten Informationen sind dazu geeignet, die Zustandsinformationen mittels der kryptografischen zweiten Informationen zu verifizieren. So sind die dem ersten Verkehrsteilnehmer 1 zugehörigen kryptografischen ersten Informationen entweder Verschlüsselungsinformationen oder umfassen ein Zertifikat, welches zumindest ein eindeutiges Identifizieren des ersten Verkehrsteilnehmers 1 bei einer Kommunikation ermöglichen. Die dem ersten Verkehrsteilnehmer 20 zugehörigen kryptografischen ersten Informationen werden von dem ersten Verkehrsteilnehmer 1 dem Applikationsserver 50 zu einem beliebigen Zeitpunkt bereitgestellt, beispielsweise wenn die erste Kommunikationsvorrichtung 10 in Betrieb genommen wird. Die dem ersten Verkehrsteilnehmer 1 zugehörigen kryptografischen ersten Informationen werden durch den Applikationsserver 50 gespeichert.

[0029] Durch die erste Kommunikationsvorrichtung 10 werden Positionsinformationen des ersten Verkehrsteilnehmers 1 an den Applikationsserver 50 übertragen. Dazu umfasst die erste Kommunikationsvorrichtung 10 eine Steuereinheit 13, durch welche die Positionsinformationen des ersten Verkehrsteilnehmers 1 erfasst werden, beispielsweise durch zugehörige Sensoren. Durch den zweiten Verkehrsteilnehmer 2 werden ebenfalls Positionsinformationen an den Applikationsserver 50 übertragen. Die Positionsinformationen umfassen dabei eine Position des zweiten Verkehrsteilnehmers 2.

[0030] Durch den Applikationsserver 50 wird geprüft, ob eine vordefinierte erste Bedingung erfüllt ist. Dies ist dann der Fall, wenn der erste Verkehrsteilnehmer 1 sich in einem definierten Bereich um den zweiten Verkehrsteilnehmer 2 befindet, beispielsweise sich auf 100m an den zweiten Verkehrsteilnehmer 2 annähert. Ob diese erste Bedingung erfüllt ist, kann durch den Applikationsserver 10 basierend auf den Positionsinformationen des erste Verkehrsteilnehmers 1 und den Positionsinformationen des zweiten Verkehrsteilnehmers 2 ermittelt werden. Ist die erste Bedingung erfüllt, so werden die dem ersten Verkehrsteilnehmer 1 zugehörigen kryptografischen ersten Informationen über das Funknetzwerk 40 an die zweite Kommunikationsvorrichtung 20 übertragen. Entsprechend werden die dem ersten Verkehrsteilnehmer 1 zugehörigen kryptografischen ersten Informationen über die erste Empfangseinheit 21 der zweiten Kommunikationsvorrichtung 20, bzw. eine der zweiten Kommunikationsvorrichtung 20 zugehörige Steuereinheit 23, empfangen. Ab diesem Zeitpunkt kann durch die zweite Kommunikationsvorrichtung 20 eine mittels der empfangenen kryptografischen ersten Informationen gesicherte Datenverbindung für einen gesicherten Datenaustausch mit der ersten Kommunikationsvorrichtung 10 des ersten Verkehrsteilnehmers 1 aufgebaut werden. So kann insbesondere von der Steuereinheit 23 der zweiten Kommunikationsvorrichtung 20 verifiziert werden, ob die von der ersten Kommunikationsvorrichtung 10 des ersten Verkehrsteilnehmers 1 empfangenen Zustandsinformationen tatsächlich von der ersten Kommunikationsvorrichtung 10 des ersten Verkehrsteilnehmers 1 ausgesendet wurden.

[0031] Es wird darauf hingewiesen, dass die vordefinierte erste Bedingung hier beispielhaft gewählt ist. Alternative Bedingungen könnten beispielsweise derart definiert sein, dass kryptografische erste Informationen des ersten Verkehrsteilnehmers 1 dann an die zweite Kommunikationsvorrichtung 20 übertragen werden, wenn diese von zweiten Kommunikationsvorrichtung 20 angefordert werden, beispielsweise, weil ein direkt gesendetes Signal von der ersten Kommunikationsvorrichtung des ersten Verkehrsteilnehmers 1 empfangen wird. Es ist jegliche erste Bedingung vorteilhaft, welche darauf schließen lässt, dass ein Datenaustausch zwischen der ersten Kommunikationsvorrichtung 10 und der zweite Kommunikationsvorrichtung 20 über die direkte Funkverbindung, also die Funkverbindung zweiter Art, erfolgen soll.

[0032] Durch die Steuereinheit 23 der zweiten Kommunikationsvorrichtung 20 werden die Zustandsinformationen, beispielsweise Positions- und/oder Bewegungsinformationen des ersten Verkehrsteilnehmers 1, über die zweite Sendeeinheit 22 der zweiten Kommunikationsvorrichtung 20 empfangen. Die Positions- und/oder Bewegungsinformationen sind dabei mittels der empfangenen kryptografischen Informationen des ersten Verkehrsteilnehmers 1 gesichert, insbesondere signiert, und können somit zuverlässig dem ersten Verkehrsteilnehmer 1 zugeordnet werden.

[0033] Die von dem ersten Verkehrsteilnehmer 1 empfangenen Zustandsinformationen des ersten Verkehrsteilnehmers 1 werden entweder durch die zweite Kommunikationsvorrichtung 20 ausgewertet oder zusammen mit eigenen Positions- und/oder Bewegungsinformationen der zweiten Kommunikationsvorrichtung 20 an den Applikationsserver 50 übertragen. Basierend auf den Zustandsinformationen des ersten Verkehrsteilnehmers 20 können Warnungen durch die zweite Kommunikationsvorrichtung 20 ausgegeben werden, welche beispiels-

weise eine Kollisionswarnung ermöglichen, wenn eine Kollision zwischen dem ersten und dem zweiten Verkehrsteilnehmer 1, 2 bevorstehen könnte. Die entsprechende Auswertung erfolgt bevorzugt durch die zweite Kommunikationsvorrichtung 20 oder alternativ durch den Applikationsserver 50, wobei entsprechende Informationen von dem Applikationsserver 50 an die zweite Kommunikationsvorrichtung 20 übertragen werden, wenn die Auswertung durch den Applikationsserver 50 erfolgt.

[0034] Durch den Applikationsserver 50 wird das Übertragen der dem ersten Verkehrsteilnehmer 20 zugehörigen kryptografischen ersten Informationen an die zweite Kommunikationsvorrichtung 20 in Reaktion auf ein Vorliegen einer vordefinierten zweiten Bedingung unterbunden. So kann beispielsweise eine Auswertung durch den Applikationsserver 50 erfolgen, welche darauf schließen lässt, ob durch den ersten Verkehrsteilnehmer 1 zuverlässige Zustandsinformationen bereitgestellt werden. Ob die Zustandsinformationen zuverlässig sind oder nicht kann entweder basierend auf den Zustandsinformationen selbst oder basierend auf den kryptografischen ersten Informationen erfolgen. So kann beispielsweise von unzuverlässigen Zustandsinformationen ausgegangen werden, wenn die kryptografischen ersten Informationen ein ungültiges Zertifikat umfassen oder die Zustandsinformationen eine unrealistische Bewegung des ersten Verkehrsteilnehmers 1 anzeigen. Lässt diese Auswertung darauf schließen, dass die dem ersten Verkehrsteilnehmer 1 zugehörigen Zustandsinformationen, beispielsweise von diesem bereitgestellten Positions- und/oder Bewegungsinformationen, nicht zuverlässig erscheinen, so kann durch den Applikationsserver 50 entschieden werden, dass die kryptografischen ersten Informationen des ersten Verkehrsteilnehmers 1 nicht an die zweite Kommunikationsvorrichtung 20 weitergeleitet werden. Als zweite Bedingung ist jegliche Bedingung geeignet, die auf eine eingeschränkte Vertrauenswürdigkeit des ersten Verkehrsteilnehmers 2 schließen lässt.

[0035] Liegen der zweiten Kommunikationsvorrichtung 20 keine dem Verkehrsteilnehmer 1 zugehörigen kryptografischen erste Informationen vor, so können empfangene Zustandsinformationen nicht verifiziert werden. In diesem Falle kann durch die zweite Kommunikationsvorrichtung 20 entschieden werden, ob die von dem ersten Verkehrsteilnehmer 1 empfangenen Zustandsinformationen für bestimmte Unterstützungsfunktionen genützt werden, indem diese beispielsweise nicht an den Applikationsserver 10 übertragen werden oder bei einer lokalen Auswertung nicht berücksichtigt werden. Es werden insbesondere empfangene Zustandsinformationen abhängig davon, ob diese verifiziert werden konnten, für unterschiedliche Unterstützungsfunktionen genutzt. Dies umfasst auch, dass Zustandsinformationen, die nicht verifiziert werden konnten, für keine Unterstützungsfunktion genutzt werden. Es wird somit beispielsweise ermöglicht, dass ein Anwender der zweiten Kommunikationsvorrichtung 20 entscheidet, ob dieser Kollisionswarnungen hinsichtlich des ersten Verkehrsteilnehmers 1 dargestellt bekommt. Optional können auch sicherheitsrelevante Unterstützungsfunktionen nur dann ermöglicht werden, wenn die Zustandsinformationen verifiziert werden konnten.

[0036] Bevorzugt werden von der zweiten Kommunikationsvorrichtung 20 kryptografische Informationen des zweiten Verkehrsteilnehmers an den Applikationsserver 10 übertragen. Zudem werden optional auch Zustandsinformationen des zweiten Verkehrsteilnehmers 2 mit zugehörigen kryptografische Informationen an die erste Kommunikationsvorrichtung 10 übertragen. Das Übertragen von Zustandsinformationen kann somit von dem zweiten Verkehrsteilnehmer 2 zu dem ersten Verkehrsteilnehmer 1 in gleicher Weise erfolgen, wie dies zuvor für das Übertragen von Zustandsinformationen von dem ersten Verkehrsteilnehmer 1 zu dem zweiten Verkehrsteilnehmer 2 beschrieben wurde.

[0037] In **Fig.** 1 sind die im Rahmen des Informationssystems genutzten Datenverbindungen dargestellt. So wird eine erste Datenverbindung 31 über das Funknetzwerk 40 von dem ersten Verkehrsteilnehmer 1 zu dem Applikationsserver 50 etabliert. Über diese erste Datenverbindung 31 können die kryptografischen ersten Informationen des ersten Verkehrsteilnehmers 1 an den Applikationsserver 50 übertragen werden.

[0038] Eine zweite Datenverbindung 32 wird zwischen dem Applikationsserver 50 und dem zweiten Verkehrsteilnehmer 2 über das Funknetzwerk 40 etabliert. Über die zweite Datenverbindung 32 können die kryptografischen ersten Informationen des ersten Verkehrsteilnehmers 1 von dem zweiten Verkehrsteilnehmer 2 empfangen werden.

[0039] Es wird eine dritte Datenverbindung 33 zwischen dem ersten Verkehrsteilnehmer 1 und dem zweiten Verkehrsteilnehmer 2 etabliert, über welche die von dem ersten Verkehrsteilnehmer 1 ausgesendeten Zustandsinformationen zusammen mit den kryptografischen zweiten Informationen durch den zweiten Verkehrsteilnehmer 2 empfangen werden können. Die dritte Datenverbindung 33 ist dabei eine gesicherte Datenverbindung, so dem zweiten Verkehrsteilnehmer 2 die dafür notwendigen zugehörigen kryptografischen ersten Informationen des ersten Verkehrsteilnehmers 1 vorliegen, um dies zu verifizieren.

[0040] Es wird optional eine vierte Datenverbindung 34 zwischen dem ersten Verkehrsteilnehmer 1 und dem zweiten Verkehrsteilnehmer 2 etabliert, über welche von dem zweiten Verkehrsteilnehmer 2 ausgesendete Zustandsinformationen zusammen mit kryptografischen Informationen durch den ersten Verkehrsteilnehmer 2 empfangen werden können. Die vierte Datenverbindung 34 ist dabei optional eine gesicherte Datenverbindung, welche in entsprechender Weise gesichert wurde, wie auch die dritte Datenverbindung 33.

[0041] Es werden somit die kryptografischen Informationen für einen gesicherten Datenaustausch mittels einer direkten Funkverbindung über eine nicht direkte Funkverbindung, hier über das Funknetzwerk 40, ausgetauscht. Dadurch wird es ermöglicht, dass kryptografische Informationen bereits dann ausgetauscht werden, wenn noch keine direkte Funkverbindung zwischen dem ersten Verkehrsteilnehmer 1 und dem zweiten Verkehrsteilnehmer 2 erfolgen kann. Somit wird ein besonders reaktionsschnelles System geschaffen. Auch wird es ermöglicht, dass kryptografischen erste Informationen durch den Applikationsserver 50 nur dann weitergeleitet werden, wenn die entsprechende Quelle als vertrauenswürdig angesehen wird. Dabei wird jedoch die zweite Kommunikationsvorrichtung 20 nicht in ihrer Entscheidungsfreiheit eingeschränkt.

[0042] **Fig.** 2 zeigt ein beispielhaftes Ablaufdiagramm für ein erfindungsgemäßes Verfahren 100 für eine Kommunikation zwischen dem ersten Verkehrsteilnehmer 1 und dem zweiten Verkehrsteilnehmer 2.

[0043] In einem ersten Verfahrensschritt 101 erfolgt dabei ein Übertragen von dem ersten Verkehrsteilnehmer 1 zugehörigen kryptografischen ersten Informationen von dem ersten Verkehrsteilnehmer an den zweiten Verkehrsteilnehmer 2 mittels der Funkverbindung erster Art.

[0044] Ferner erfolgt in einem zweiten Verfahrensschritt 102 ein Übertragen von dem ersten Verkehrsteilnehmer 1 zugehörigen Zustandsinformationen, hier beispielsweise Positions- und/oder Bewegungsinformationen, zusammen mit den kryptografischen zweiten Informationen von dem ersten Verkehrsteilnehmer 1 an den zweiten Verkehrsteilnehmer 2 über die Funkverbindung zweiter Art. Die kryptografischen ersten Informationen sind dazu geeignet, die Zustandsinformationen mittels der kryptografischen zweiten Informationen zu verifizieren.

[0045] In einem dritten Verfahrensschritt 103 erfolgt ein Verifizieren der Zustandsinformationen basierend auf den kryptografischen ersten Informationen mittels der kryptografischen zweiten Informationen durch den zweiten Verkehrsteilnehmer 2, also durch die zweite Kommunikationsvorrichtung. In der mit **Fig.** 1 gezeigten Ausführungsform erfolgt ein Datenaustausch über ein Funknetzwerk 40 und einen zwischengeschalteten Applikationsserver 50. In alternativen Ausführungsformen erfolgt eine Kommunikation zwischen der ersten Sendeeinheit 11 der ersten Kommunikationsvorrichtung 10 und der ersten Empfangseinheit 21 der zweiten Kommunikationsvorrichtung 20 ebenfalls über eine direkte Funkverbindung. Insbesondere falls diese direkte Funkverbindung zwischen der ersten Sendeeinheit 11 der ersten Kommunikationsvorrichtung 10 und der ersten Empfangseinheit 21 der zweiten Kommunikationsvorrichtung 20 eine größere Reichweite als die Funkverbindung zweiter Art aufweist, können die kryptografischen ersten Informationen ebenfalls bereitgestellt werden, bevor die Zustandsinformationen zusammen mit den zweiten Informationen empfangen werden.

[0046] **Fig.** 3 zeigt eine weitere beispielhafte Ausführungsform der Erfindung, wobei der Informationsfluss im Wesentlichen der in **Fig.** 2 gezeigten Ausführungsform entspricht. Dabei ist jedoch die Funkverbindung erster Art, hier die eine fünfte Datenverbindung 35, eine direkte Kommunikationsverbindung zwischen der ersten Sendeeinheit 11 und der ersten Empfangseinheit 21. Optional kann durch die erste Kommunikationsvorrichtung 10 und/oder die zweite Kommunikationsvorrichtung 20 ein zusätzlicher Datenaustausch mit dem Kommunikationsserver erfolgen. Auch in dieser Ausführungsform können die kryptografischen ersten Informationen der zweiten Kommunikationsvorrichtung 20 bereitgestellt werden, bevor die dem ersten Verkehrsteilnehmer 1 zugehörige Zustandsinformationen zusammen mit den kryptografischen zweiten Informationen empfangen werden. Somit können die empfangenen Zustandsinformationen mittels der kryptografischen zweiten Informationen und basierend auf den kryptografischen ersten Informationen verifiziert werden, sobald die Zustandsinformationen von der zweiten Kommunikationsvorrichtung 20 empfangen werden. Eine Reichweite der fünften Datenverbindung 35 ist dabei größer als eine Reichweite der dritten Datenverbindung 33.

[0047] Der Ansatz, in dem dieselben C-V2X Technologien an ein Fahrrad gebracht werden, die auch im Auto verwendet werden, ist vergleichsweise aufwändig und teuer. Zudem wird diese Technologie nach aktuellem Stand nicht in allen Regionen der Welt flächendeckend zum Einsatz kommen. Außerdem ist die Bandbreite der C-V2X Direktkommunikation sehr begrenzt und seitens der Automobilwelt gibt es Widerstände, auch Vulnerable Road User (wie Fahrräder oder Fußgänger) in diesem engen Frequenzband funken zu lassen, da befürchtet wird, dass die Frequenzbänder damit überfrachtet werden und Sicherheitsanwendungen zwischen Fahrzeugen

und Infrastruktur dadurch in Mitleidenschaft gezogen werden.

[0048] Daher wird durch das erfindungsgemäße Verfahren vorgeschlagen, parallel eine LongRange-Kommunikation (4G/5G/LoRaWaN) mit einer ShortRange-Kommunikation (z.B. BLE) zu nutzen. Die LongRange-Kommunikation ist dabei die Komunikation über die erste Sende- und Empfangseinheit. Die ShortRange-Kommunikation ist dabei die Komunikation über die zweite Sende- und Empfangseinheit.

[0049] Die LongRange-Kommunikation wird dabei optional für weniger zeitkritische Dinge wie Erhöhung der Wahrnehmung (gegenseitige Präsenzinfo bei Fahrrad und Auto) oder auch Kollisionswarnungen genutzt. Zudem wird die LongRange-Kommunikation ebenso als Kanal zur Absicherung der Sicherheit und als einer von zwei Kanälen für sicherheitskritischere Anwendungen genutzt, wobei außerdem auch langreichweitig oder „langsame“ Informationen (wie Warnungen vor quasistatischen Gefahren wie Glatteisstellen, Wetter, Unfälle, Straßensperrungen etc.) über die LongRange-Kommunikation einfliessen.

[0050] Die ShortRange-Kommunikation wird für zeitkritische Kommunikation zwischen Fahrrad und Fahrzeug, also zwischen mobiler Einheit 1 und Verkehrsteilnehmer 20, genutzt, um hochfrequent und mit geringen Latenzen den künftigen Pfad und weitere Informationen über den Zustand des Fahrrads bzw. des Radfahrers senden zu können.

[0051] Es wird somit eine Kombination von LongRange und ShortRange Kommunikation, insbesondere 4G/5G/LoRaWaN mit BLE oder anderen kurzreichweitigen Technologien (z.B. UltraWideBand) außerhalb der in ab Rel14 vorgesehenen Sidelink-Kommunikation, geschaffen.

Dies ist vorteilhaft in mehrerlei Hinsicht:

[0052] Aus sicherheitstechnischer Sicht existieren zwei parallele und technologisch unabhängige Pfade. Forderungen hinsichtlich einer solchen Redundanz werden zunehmend lauter im Kontext von sicherheitskritischen Anwendungen (wie z.B. automatisiertes Bremsen).

[0053] Aus sicherheitstechnischer Sicht erlaubt ein zweiter, vom ersten Kanal unabhängiger (out-of-band) und vorzugsweise langreichweitiger Kanal einen Austausch von kryptographischen Informationen zur Absicherung der ShortRange Schnittstelle. Damit ermöglicht dieser Kanal die Verlagerung von Aufwand in die weniger zeitkritische und über längere Distanzen reichende Kommunikationsschnittstelle.

[0054] Der in der LongRange Kommunikation zwischengeschaltete Applikationsserver 10 (der auch bestimmt, welche anderen Verkehrsteilnehmer in der Nähe sind und an die entsprechend die Nachricht mit kryptografischen Informationen weitergeleitet werden muss), kann eine Caching-Funktion beinhalten, also beispielsweise die Zertifikate zwischenspeichern und proaktiv den Kommunikationspartnern zur Verfügung stellen, sobald ShortRange Kommunikation zu erwarten ist.

[0055] In einer vorteilhaften Ausbaustufe kann der Applikationsserver 10 darüber hinaus dazu genutzt werden, die Zertifikate nicht weiterzuleiten und somit einem Kommunikationspartner das Vertrauen entziehen, ohne die Kommunikation komplett zu unterbinden. Damit kann der Empfänger entscheiden, für welche sicherheitskritischen Reaktionen (z.B. automatisiertes Notbremsen) er die „degradierten“ Informationen aus dem ShortRange-Kanal noch nutzt oder eben nicht.

[0056] Grundlage für einen solchermaßen realisierten „Entzug“ der Zertifikate muss eine Bewertung der Vertrauenswürdigkeit der Kommunikationspartner sein, die im Hintergrund erfolgt, beispielsweise anhand einer Anomalieerkennung („dieser Verkehrsteilnehmer verhält sich seltsam, nicht passend zu seinem Profil, zu viele auf einer Stelle (Misuse) etc.). Somit lässt sich eine online Revokation umsetzen, ohne Mechanismen in der darunterliegenden PKI zu verwenden (kurzlebige Zertifikate nach ETSI können by design nicht revoziert werden). Der Vermittler im Backend „orchestriert“, damit die Vertrauenswürdigkeit der Kommunikationspartner, ohne an der Kommunikation selbst teilzunehmen.

[0057] Analog dazu lassen sich auch für ad-hoc Kommunikation Short- und LongRange Kommunikation kombinieren, ohne vermittelnde Zwischenstelle, beispielsweise über eine Kombination aus PC5/WiFi-p mit Bluetooth, sodass über Bluetooth nur der Austausch von Hashes notwendig ist. Stattdessen werden notwendige Informationen über weitere Distanzen vorprovisioniert.

[0058] Anwendungen, die keine sehr kleinen Latenzen brauchen (wie z.B. eine Warnung oder Information im Zeitbereich >1.5s vor einer Gefahrensituation), können bidirektional über die LongRange-Schnittstelle und insbesondere über den Applikationsserver 10 erfolgen, d.h. sowohl die mobile Einheit 1 als auch andere Verkehrsteilnehmer können die Fahrer vorwarnen.

[0059] Anwendungen, die auf sehr kleine Latenzen und hohe Verfügbarkeit angewiesen sind (wie z.B. die Unterstützung eines automatisierten Bremseingriffes), profitieren von den kurzen Latenzen der

Direktkommunikation (ShortRange), plus der erhöhten Sicherheit über die Zweikanaligkeit.

[0060] Da es bei sicherheitsrelevanten automatisierten Eingriffen v.a. um Eingriffe auf der Seite des Verkehrsteilnehmers 10 geht (wie z.B. automatisierte Bremseingriffe, AEB), reicht für die ShortRange Communication auch eine Unidirektionale Kommunikation. In beiden Fällen kann eine ShortRange Kommunikation erfolgen, ermöglicht durch intelligentes Caching, auch wenn der LongRange Kanal nicht durchgehend verfügbar ist.

[0061] Vorteilhaft ist außerdem, dass mit dieser Kommunikation die geringe Bandbreite einer möglichen Sidelink-Kommunikation nicht belastet wird. Dies kann zu mehr Akzeptanz seitens der Kraftfahrzeuge führen, weil die sicherheitskritische Kommunikation zwischen unterschiedlichen Kraftfahrzeugen dann nicht durch VRUs beeinträchtigt wird.

[0062] Es ist somit bei dem beschriebenen Informationssystem ein Fahrrad, welches die mobile Einheit 1 umfasst, über die LongRange Verbindung mit einem Backend (dem Applikationsserver 10) verbunden, beispielsweise mindestens auf einer Zeitskala von einigen Sekunden. Sollte sich das Fahrrad auf eine Gefahrenstelle (statisch oder dynamisch) zubewegen, können Informationen / Warnungen an das Fahrrad übermittelt werden.

[0063] Im Bedarfsfall kann die Kommunikationsfrequenz erhöht werden, jedoch wird es Einschränkungen bzgl. der Latenz geben, weshalb die LongRange Technologie (auch aufgrund ggfs. vorhandener „Funklöcher“) tendenziell nicht tauglich ist, auch eine Notbremsfunktion im Auto zu unterstützen.

[0064] Hier kommt die ShortRange Kommunikation ins Spiel, die mit geringen Latenzen und ohne Abhängigkeit von einem Mobilfunknetz mit dem Auto kommunizieren kann. Beispielsweise können via BLE mit 10Hz CAM/VAM-Nachrichten gesendet werden, die Auskunft über die eigene Position, Richtung, Geschwindigkeit, vorausberechneten Pfad in den nächsten Sekunden, Fahrertyp und -Reaktionen geben können, die dem Auto helfen, die richtigen Manöver einzuleiten.

[0065] Um nicht auf diesem Pfad auch vollständiges Schlüsselmaterial (die vollständigen kryptografischen Informationen) transportieren zu müssen, kann dieses auf der LongRange-Kommunikation im Vorfeld schon geschehen, sodass sich die (begrenzte) ShortRange Kommunikation auf die wesentlichen, safetyrelevanten Inhalte konzentrieren kann.

[0066] Die LongRange Kommunikation dient zusätzlich als zweiter, unabhängiger Kanal, der für Sicherheitsanwendungen sehr hilfreich (wenn nicht sogar notwendig) sein wird.

[0067] Neben der obigen schriftlichen Offenbarung wird explizit auf die Offenbarung der **Fig.** 1 bis 3 verwiesen.

Patentansprüche

1. Erste Kommunikationsvorrichtung (10) für einen ersten Verkehrsteilnehmer (1), umfassend:
- eine erste Sendeeinheit (11), welche dazu eingerichtet ist, Informationen über eine Funkverbindung erster Art zu senden,
- eine zweite Sendeeinheit (12), welche dazu eingerichtet ist, Informationen über eine Funkverbindung zweiter Art zu senden, und
- eine Steuereinheit (13) der ersten Kommunikationsvorrichtung (10), welche dazu eingerichtet ist,
- dem ersten Verkehrsteilnehmer (1) zugehörige kryptografische erste Informationen über die erste Sendeeinheit (11) zu senden, und
- dem ersten Verkehrsteilnehmer (1) zugehörige Zustandsinformationen zusammen mit kryptografischen zweiten Informationen über die zweite Sendeeinheit (12) zu senden, wobei die kryptografischen ersten Informationen dazu geeignet sind, die Zustandsinformationen mittels der kryptografischen zweiten Informationen zu verifizieren.

2. Erste Kommunikationsvorrichtung (10) gemäß Anspruch 1,
- wobei die erste Sendeeinheit (11) dazu eingerichtet ist, Informationen über ein Funknetzwerk (40) an einen Kommunikationsserver (50) zu senden, und die Steuereinheit (13) der ersten Kommunikationsvorrichtung (10) dazu eingerichtet ist, die kryptografischen ersten Informationen an den Kommunikationsserver (50) zu senden, und
- wobei die zweite Sendeeinheit (12) dazu eingerichtet ist, die Zustandsinformationen zusammen mit den kryptografischen zweiten Informationen über eine direkte Funkverbindung an einen zweiten Verkehrsteilnehmer (2) zu senden.

3. Erste Kommunikationsvorrichtung (10) gemäß einem der voranstehenden Ansprüche, wobei die dem ersten Verkehrsteilnehmer (1) zugehörigen kryptografischen ersten Informationen ein digitales Zertifikat umfassen und die dem zweiten Verkehrsteilnehmer (2) gesendeten kryptografischen zweiten Informationen einen Hashwert umfassen, welcher basierend auf dem digitalen Zertifikat generiert wurde.

4. Erste Kommunikationsvorrichtung (10) gemäß einem der voranstehenden Ansprüche, wobei die erste Sendeeinheit (11) für eine Übertragung über eine größere Reichweite vorgesehen ist als die zweite Sendeeinheit (12), und/oder die erste Sende-

einheit (11) dazu eingerichtet ist, größere Datenpakete zu übertragen, als die zweite Sendeeinheit (12).

5. Zweite Kommunikationsvorrichtung (20) für einen zweiten Verkehrsteilnehmer (2), umfassend:
- eine erste Empfangseinheit (21), welche dazu eingerichtet ist, Informationen über eine Funkverbindung erster Art zu empfangen,
- eine zweite Empfangseinheit (22), welche dazu eingerichtet ist, Informationen über eine Funkverbindung zweiter Art zu empfangen, und
- eine Steuereinheit (23), welche dazu eingerichtet ist:
- einem ersten Verkehrsteilnehmer (1) zugehörige kryptografische erste Informationen über die erste Empfangseinheit (21) zu empfangen, und
- dem ersten Verkehrsteilnehmer (1) zugehörige Zustandsinformationen zusammen mit kryptografischen zweiten Informationen über die zweite Empfangseinheit (22) zu empfangen, und
- die Zustandsinformationen basierend auf den kryptografischen ersten Informationen mittels der kryptografischen zweiten Informationen zu verifizieren.

6. Zweite Kommunikationsvorrichtung (20) gemäß Anspruch 5,
- wobei die erste Empfangseinheit (21) dazu eingerichtet ist, Informationen über ein Funknetzwerk (40) von einem Kommunikationsserver (50) zu empfangen, und die Steuereinheit (23) der zweiten Kommunikationsvorrichtung (20) dazu eingerichtet ist, die kryptografischen ersten Informationen von dem Kommunikationsserver (50) zu empfangen, und
- wobei die zweite Empfangseinheit (22) dazu eingerichtet ist, die Zustandsinformationen zusammen mit den kryptografischen zweiten Informationen über eine direkte Funkverbindung von dem ersten Verkehrsteilnehmer (1) zu empfangen.

7. Zweite Kommunikationsvorrichtung (20) gemäß einem der voranstehenden Ansprüche 5 oder 6, wobei die dem ersten Verkehrsteilnehmer (1) zugehörigen kryptografischen ersten Informationen ein digitales Zertifikat umfassen und die dem zweiten Verkehrsteilnehmer (2) gesendeten kryptografischen zweiten Informationen einen Hashwert umfassen, welcher basierend auf dem digitalen Zertifikat generiert wurde.

8. Zweite Kommunikationsvorrichtung (20) gemäß einem der voranstehenden Ansprüche 5 bis 7, wobei die erste Empfangseinheit (21) für eine Übertragung über eine größere Reichweite vorgesehen ist als die zweite Empfangseinheit (22), und/oder die erste Empfangseinheit (21) dazu eingerichtet ist, größere Datenpakete zu übertragen als die zweite Empfangseinheit (22).

9. Zweite Kommunikationsvorrichtung (20) gemäß einem der voranstehenden Ansprüche 5 bis 8, wobei die Steuereinheit (23) dazu eingerichtet ist, die über die zweite Empfangseinheit (22) von dem ersten Verkehrsteilnehmer (1) empfangenen Zustandsinformationen abhängig davon, ob die Zustandsinformationen mittels der kryptografischen zweiten Informationen erfolgreich verifiziert werden können, für unterschiedliche Unterstützungsfunktionen zu nutzen.

10. Kommunikationssystem, umfassend die erste Kommunikationsvorrichtung (10) gemäß einem der voranstehenden Anspruch 2 und/oder die zweite Kommunikationsvorrichtung (20) gemäß Anspruch 6, ferner umfassend den Kommunikationsserver (50), wobei der Kommunikationsserver (50) dazu eingerichtet ist, die dem ersten Verkehrsteilnehmer (1) zugehörigen kryptografischen ersten Informationen in Reaktion darauf an die zweite Kommunikationsvorrichtung (20) zu übertragen, dass eine vordefinierte erste Bedingung erfüllt ist, wobei die vordefinierte erste Bedingung insbesondere dann erfüllt ist, wenn dem Kommunikationsserver (50) eine Information vorliegt, die auf einen zu erwartenden Datenaustausch zwischen der erste Kommunikationsvorrichtung (10) und der zweiten Kommunikationsvorrichtung (20) über die Funkverbindung zweiter Art schließen lässt.

11. Kommunikationssystem gemäß Anspruch 10, wobei der Kommunikationsserver (50) dazu eingerichtet ist, das Übertragen der dem ersten Verkehrsteilnehmer (1) zugehörigen kryptografischen ersten Informationen an die zweite Kommunikationsvorrichtung (20) in Reaktion auf ein Vorliegen einer vordefinierten zweiten Bedingung zu unterbinden, wobei die vordefinierte zweite Bedingung insbesondere dann erfüllt ist, wenn dem Kommunikationsserver (50) eine Information vorliegt, die auf eine eingeschränkte Vertrauenswürdigkeit des ersten Verkehrsteilnehmers (1) schließen lässt.

12. Verfahren (100) für eine Kommunikation zwischen einem ersten Verkehrsteilnehmer (1) und einem zweiten Verkehrsteilnehmer (2), umfassend:
- Übertragen (101) von dem ersten Verkehrsteilnehmer (1) zugehörigen kryptografischen ersten Informationen von dem ersten Verkehrsteilnehmer (1) an den zweiten Verkehrsteilnehmer (2) mittels einer Funkverbindung erster Art (31),
- Übertragen (102) von dem ersten Verkehrsteilnehmer (1) zugehörigen Zustandsinformationen zusammen mit kryptografischen zweiten Informationen von dem ersten Verkehrsteilnehmer (1) an den zweiten Verkehrsteilnehmer (2) über eine Funkverbindung zweiter Art, wobei die kryptografischen ersten Informationen dazu geeignet sind, die Zustandsinformationen mittels der kryptografischen zweiten Informationen zu verifizieren,

- Verifizieren (103) der Zustandsinformationen basierend auf den kryptografischen ersten Informationen mittels der kryptografischen zweiten Informationen durch den zweiten Verkehrsteilnehmer.

Es folgen 2 Seiten Zeichnungen

Anhängende Zeichnungen

Fig. 1

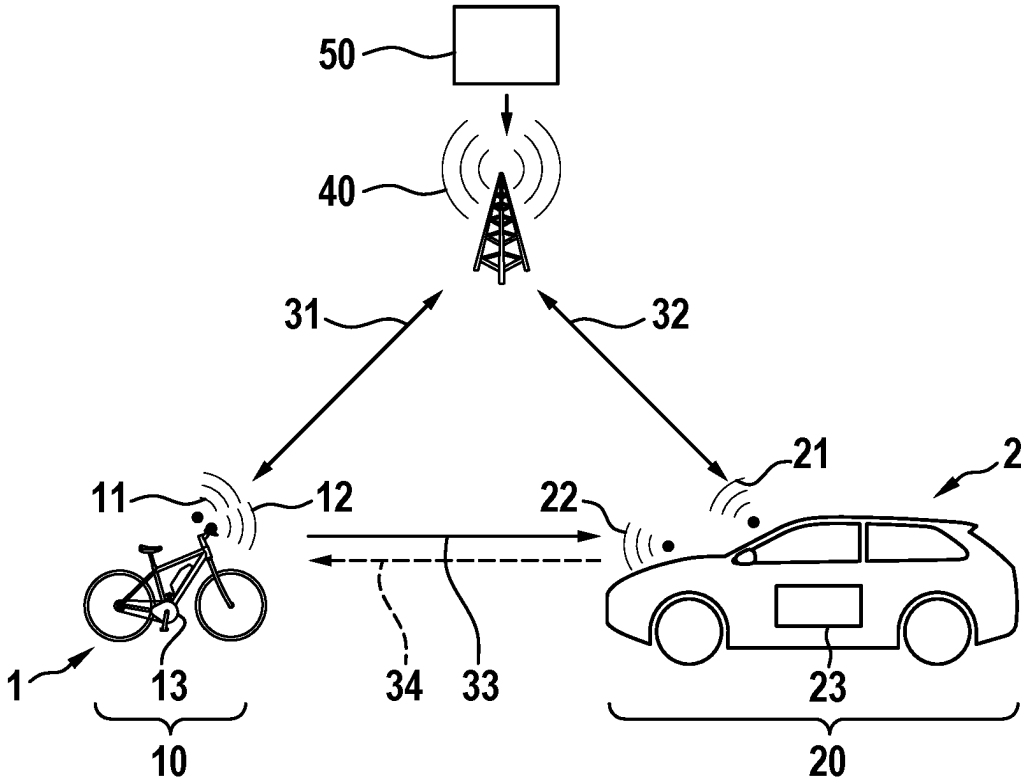


Fig. 2

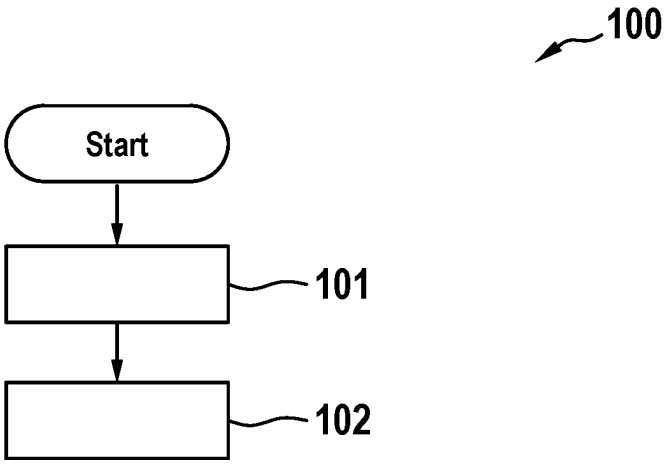
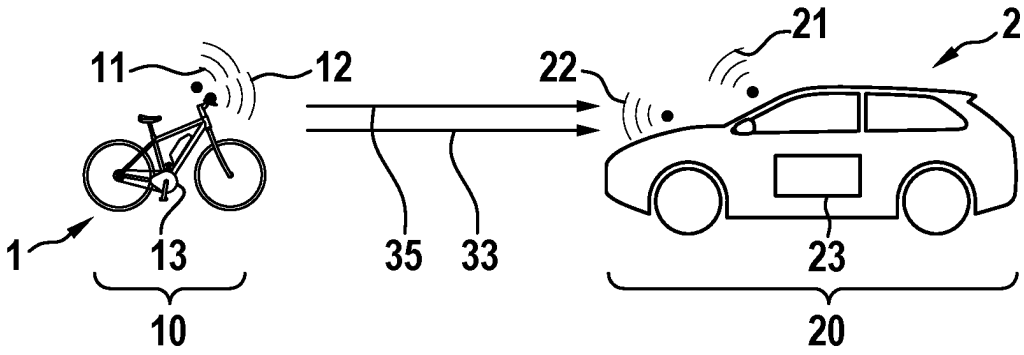


Fig. 3



 Das Dokument wurde durch die Firma Luminess hergestellt.