(19) Deutsches Patent- und Markenamt

(10) **DE 10 2015 225 787 A1** 2017.06.22

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2015 225 787.8**
(22) Anmeldetag: **17.12.2015**
(43) Offenlegungstag: **22.06.2017**

(51) Int Cl.: ***H04L 9/32*** (2006.01)

(71) Anmelder:
VOLKSWAGEN AKTIENGESELLSCHAFT, 38440 Wolfsburg, DE

(72) Erfinder:
Baade, Marco, 31848 Bad Münder, DE; Winkelvos, Timo, 38104 Braunschweig, DE; Gierds, Christian, 10243 Berlin, DE; Tschache, Alexander, 38440 Wolfsburg, DE

(56) Ermittelter Stand der Technik:

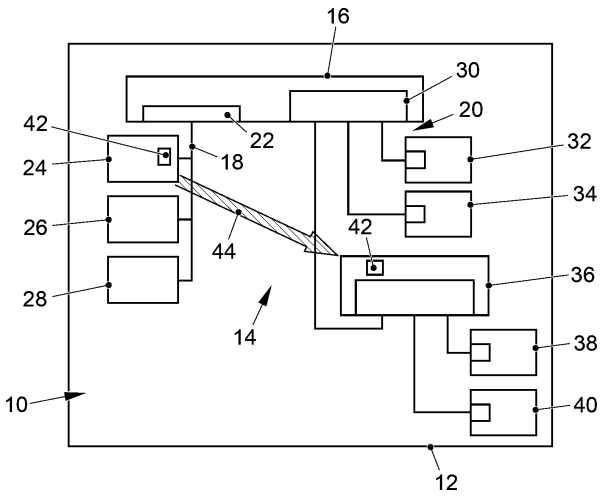
WO	**2005/ 115 809**	**A1**
WO	**2005/ 116 834**	**A1**

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren und Vorrichtung zur Empfängerauthentifikation in einem Fahrzeugnetzwerk**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Empfängerauthentifikation in einem Fahrzeugnetzwerk (14; 140) mit mindestens einem Sender (36; 160) und mindestens einem Empfänger (24; 240).
Es sind Schritte vorgesehen, des Sendens eines Authentizitätsmerkmals durch den Empfänger (24; 240); des Empfangens des Authentizitätsmerkmals durch den Sender (36; 160); und des Prüfens der Authentizität des Empfängers (24; 240) anhand des Authentizitätsmerkmals durch den Sender (36; 160).
Der Erfindung liegt die Aufgabe zugrunde, die Authentizitätsprüfung eines Empfängers zu vereinfachen.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Empfängerauthentifikation in einem Fahrzeugnetzwerk, eine Vorrichtung zur Empfängerauthentifikation in einem Fahrzeugnetzwerk sowie ein Fahrzeug.

[0002] Sender von kritischen Informationen in einem heutigen Fahrzeugnetzwerk oder Fahrzeugbussystem können nicht validieren, ob der Empfänger der Nachrichten einen integren Zustand hat. Dies ist insbesondere dann kompliziert, wenn der Empfänger eigentlich keine Nachrichten an den Sender schickt, was bei einer unidirektionalen Kommunikation zum Beispiel im Fahrzeugverbund häufig der Fall ist. Zum Beispiel könnten manipulierte Geräte eingebaut werden, ohne dass der Sender dies feststellen kann.

[0003] Eine gegenseitige Authentifizierung, wie durch TLS oder IPSec, ist in diesem und auch weiteren Anwendungsbereichen aufgrund von Ressourcenbeschränkungen der Teilnehmer nicht umsetzbar.

[0004] WO 2005/115809 A1 offenbart ein Verfahren zur Authentisierung einer fahrzeugexternen Vorrichtung, bei dem in dem Bussystem eine Authentisierungsvorrichtung vorgesehen ist, welche eine Authentisierungsanfrage an die fahrzeugexterne Vorrichtung übermittelt, um eine asymmetrisch verschlüsselte Kommunikation aufzubauen

[0005] WO 2005/116834 A1 offenbart ein Verfahren zur Authentisierung von Steuergeräten in einem Bussystem eines Kraftfahrzeugs, wobei ein erstes Steuergerät über das Bussystem eine Authentisierungsanfrage an eine Authentisierungsvorrichtung übermittelt, derart dass die Kommunikation mit einem symmetrischen Schlüssel gesichert wird.

[0006] Der Erfindung liegt nun die Aufgabe zugrunde, die Authentizitätsprüfung eines Empfängers zu vereinfachen.

[0007] Diese Aufgabe wird gelöst durch ein Verfahren gemäß Anspruch 1, eine Vorrichtung gemäß Anspruch 8 beziehungsweise ein Fahrzeug gemäß Anspruch 12.

[0008] Das erfindungsgemäße Verfahren zur Empfängerauthentifikation in einem Fahrzeugnetzwerk mit mindestens einem Sender und mindestens einem Empfänger umfasst die Schritte:

– Senden eines Authentizitätsmerkmals durch den Empfänger;

– Empfangen des Authentizitätsmerkmals durch den Sender; und

– Prüfen der Authentizität des Empfängers anhand des Authentizitätsmerkmals durch den Sender.

[0009] Das erfindungsgemäße Verfahren hat den Vorteil, dass es ressourcenschonend ist und daher auch auf Teilnehmern mit geringer Rechenleistung ausgeführt werden kann. Zum ist es gut skalierbar bezüglich Umfang und Anzahl der Teilnehmer. Das Verfahren kann auf unterschiedlichen Bus- und Protokolltechnologien eingesetzt werden und beeinflusst nicht die bestehenden Botschaften und Signale. Die Gefahr durch informationstechnische Manipulationen, welche mit der steigenden Digitalisierung verbunden ist, kann durch das vorgeschlagene Verfahren verringert werden, da direkt der Empfänger authentifiziert wird und nicht wie meist üblich die Nachrichten zwischen Sender und Empfänger. Dies erlaubt die Identifizierung nicht authentischer Netzwerkteilnehmer. Diese Identifizierung oder Authentizitätsprüfung wird zum Beispiel mit einer Authentizitätsbotschaft vor dem Senden der eigentlichen Nachrichten ausgeführt, so dass der Sender der eigentlichen Nachricht einen Mechanismus für die Authentifizierung des oder der Empfänger seiner Daten zur Verfügung gestellt bekommt. Das Fahrzeugnetzwerk kann zum Beispiel ein Bussystem, wie ein CAN-Bus, sein.

[0010] Das Authentizitätsmerkmal kann eine Signatur sein. Eine Signatur ist bereits vorhanden oder einfach zu erstellen, was die Umsetzung des Verfahrens erleichtert. Statt einer Signatur kann zum Beispiel eine konstante Zahl als Authentizitätsmerkmal verwendet werden, die dann im Sender und im Empfänger vorhanden ist.

[0011] Das Authentizitätsmerkmal kann auf zuvor in den mindestens einen Sender und den mindestens einen Empfänger symmetrischen Schlüsseln basieren. Oft sind derartige Schlüssel, zum Beispiel für die Verschlüsselung der Kommunikation in dem Fahrzeugnetzwerk bereits vorhanden, so dass kein weiterer Aufwand betrieben werden muss. Im Vergleich zu asymmetrischen Verschlüsselungsverfahren ist der Rechenaufwand bei dem hier vorgeschlagenen symmetrischen Verschlüsselungsverfahren geringer. Bei ausreichender Infrastruktur kann auch ein asymmetrisches Verschlüsselungsverfahren eingesetzt werden.

[0012] Das Authentizitätsmerkmal kann zyklisch gesendet werden. Ein zyklisches Aussenden eignet sich insbesondere für Systeme mit mehreren Sendern und Empfängern. Da die das Authentizitätsmerkmal enthaltene Authentizitätsbotschaft keine weitere Datenlast hat, führt eine zyklische Versendung nicht zu einer Verringerung der Übertragungsbandbreite.

[0013] Das Authentizitätsmerkmal kann auf Anfrage gesendet werden. Hierbei kann zum Beispiel ein Sender oder ein Busmaster dediziert das Authentizitätsmerkmal eines, mehrerer oder aller Empfänger eines Systems anfordern. Dies kann zum Beispiel vor dem

Senden einer Nachricht oder für eine Bestandsaufnahme oder Überprüfung des Systems geschehen. Die zyklische Sendung und die Sendung auf Anfrage können auch kombiniert werden.

[0014] Es kann vorgesehen sein, dass der mindestens eine Sender und der mindestens eine Empfänger Steuergeräte sind. In Fahrzeugen sind dies typische Busteilnehmer, die auch, zum Beispiel im Rahmen einer Reparatur, ausgetauscht werden können. Dadurch ändert sich das System oder der Verbund, so dass die Authentifizierung des oder der Steuergeräte die Sicherheit erhöht.

[0015] Es kann weiter vorgesehen sein, dass eine Nachricht durch den Sender an den Empfänger nur bei erfolgter Authentifizierung gesendet wird. Dadurch wird verhindert, dass ein nicht authentifizierter Teilnehmer Daten oder Nachrichten von dem Sender erhält. Auf diese Weise kann ein nicht erwünschter Abfluss von Daten oder Informationen verhindert werden.

[0016] Die erfindungsgemäße Vorrichtung zur Empfängerauthentifikation in einem Fahrzeugnetzwerk mit mindestens einem Sender und mindestens einem Empfänger, dadurch gekennzeichnet, dass der mindestens eine Empfänger eingerichtet ist, ein Authentizitätsmerkmal zu senden und dass der mindestens eine Sender eingerichtet ist, die Authentizität des Empfängers anhand des Authentizitätsmerkmals zu prüfen. Es gelten die gleichen Vorteile und Modifikationen wie zuvor beschrieben.

[0017] Der mindestens eine Sender und der mindestens eine Empfänger können Steuergeräte sein. In Fahrzeugen sind dies typische Busteilnehmer, die auch, zum Beispiel im Rahmen einer Reparatur, ausgetauscht werden können. Dadurch ändert sich das System oder der Verbund, so dass die Authentifizierung des oder der Steuergeräte die Sicherheit erhöht.

[0018] Der mindestens eine Sender kann ein Busmaster des Fahrzeugnetzwerkes sein. Der Busmaster kann durch den Empfang von Authentizitätsmerkmalen einzelner oder aller Teilnehmer beziehungsweise Empfänger diese authentifizieren. Der Busmaster kann eine entsprechende Liste oder Datenbank anlegen beziehungsweise pflegen. Die Teilnehmer des Busses können auf diese Liste zugreifen oder der Busmaster kann die Kommunikation zentral steuern.

[0019] Der mindestens eine Sender kann eingerichtet sein, bei erfolgreicher Prüfung eine Nachricht an den mindestens einen Empfänger zu senden. Im Falle einer nicht erfolgreichen Prüfung erfolgt keine Sendung. Zudem kann der Empfänger in eine Liste nicht authentifizierter Teilnehmer aufgenommen werden, um jegliche Kommunikation mit diesem Teilnehmer zu unterbinden, bis eine erfolgreiche Authentifizierung erfolgt oder eventuell der Empfänger ausgetauscht wurde.

[0020] Das erfindungsgemäße Fahrzeug mit einem Fahrzeugnetzwerk mit mindestens einem Sender und mindestens einem Empfänger umfasst eine Vorrichtung wie zuvor beschrieben. Es gelten die gleichen Vorteile und Modifikationen wie zuvor beschrieben.

[0021] Weitere bevorzugte Ausgestaltungen der Erfindung ergeben sich aus den übrigen, in den Unteransprüchen genannten Merkmalen.

[0022] Die verschiedenen in dieser Anmeldung genannten Ausführungsformen der Erfindung sind, sofern im Einzelfall nicht anders ausgeführt, mit Vorteil miteinander kombinierbar.

[0023] Die Erfindung wird nachfolgend in Ausführungsbeispielen anhand der zugehörigen Zeichnungen erläutert. Es zeigen:

[0024] Fig. 1 eine schematische Darstellung einer ersten Vorrichtung zur Empfängerauthentifikation in einem Fahrzeugnetzwerk; und

[0025] Fig. 2 eine schematische Darstellung einer zweiten Vorrichtung zur Empfängerauthentifikation in einem Fahrzeugnetzwerk.

[0026] Fig. 1 zeigt eine Vorrichtung **10** zur Empfängerauthentifikation in einem Fahrzeug **12**. Die Vorrichtung **10** dient zur Authentifizierung von Empfängern in einem Netzwerk **14** des Fahrzeugs **12**. Das Fahrzeug **12** kann zum Beispiel ein PKW, LKW, Motorrad, Bus oder Bahn sein. Als Fahrzeug werden hier sämtliche Land-, Luft- und Wasserfahrzeuge angesehen.

[0027] Das Netzwerk **14** hat einen Busmaster **16**, der hier in Form eines Gateways zwischen einem Bussystem **18** und einer Netztopographie **20**. Das Bussystem **18** ist in diesem Beispiel ein CAN Bus oder ein anderer Feldbus. Der Busmaster **16** agiert als Busmaster für das Bussystem **18** und enthält eine entsprechende Bus-Schnittstelle **22**. An das Bussystem **18** sind mehrere Steuergeräte **24**, **26** und **28** angeschlossen, so dass sie mit der Bus-Schnittstelle **22** kommunizieren können.

[0028] Zur Kommunikation mit der Netztopographie **20** hat der Busmaster **16** eine Netz-Schnittstelle **30**, zum Beispiel in Form eines Switches, Routers oder Hubs. Die Netz-Schnittstelle **30** kontrolliert die Netztopographie **20**, zum Beispiel in Form eines DNS-Servers (Domain Name System). Die Netztopographie **20** kann zum Beispiel auf dem Ethernet-Standard basieren.

[0029] Zur Umsetzung zwischen den beiden Teilnetzen beziehungsweise zwischen dem Bussystem **18** und der Netztopographie **20** kann der Busmaster **16** eine Netzwerk-Bridge oder ähnliches aufweisen. Vorzugsweise enthält der Busmaster **16** einen Mikrocomputer oder ähnliches, um die anfallenden Berechnungen auszuführen.

[0030] An die Netz-Schnittstelle **30** sind direkt zwei Steuergeräte **32** und **34** sowie ein Switch **36** angeschlossen. An den Switch **36** sind wiederum zwei weitere Steuergeräte **38** und **40** angeschlossen. Der Switch **36** selbst kann auch ein Steuergerät sein. Die hier gezeigte Netzstruktur der Netztopographie **20** ist lediglich beispielhaft und kann alle technisch möglichen Kombinationen von Netzwerkkomponenten umfassen. Auch ist es möglich, dass nur ein Teilnetz, zum Beispiel das Bussystem **18**, vorhanden ist. Alternativ können auch mehr als die zwei hier dargestellten Teilnetze vorhanden sein.

[0031] Die Teilnehmer des Netzwerks **14**, das heißt die Steuergeräte **24**, **26**, **28**, **32**, **34**, **38** und **40**, der Busmaster **16** und der Switch **36** kommunizieren miteinander. Diese Kommunikation kann zum Beispiel eine symmetrische Verschlüsselung verwenden. Dazu ist in jedem Teilnehmer mindestens ein symmetrischer Schlüssel **42** vorhanden, von denen der Übersicht wegen nur zwei in dem Steuergerät **24** und dem Switch **36** dargestellt sind. Diese in diesem Beispiel bereits vorhandenen symmetrischen Schlüssel **42** werden außerdem zur Prüfung der Authentizität von Steuergeräten verwendet, wie im Folgenden erläutert wird. Die Teilnehmer beziehungsweise die Steuergeräte haben einen Authentifizierungsmechanismus für Nachrichten, mit dem sie in Kombination mit dem symmetrischen Schlüsselmaterial die Authentizität der Sender von Nachrichten überprüfen können.

[0032] In diesem Beispiel ist der Switch beziehungsweise das Steuergerät **36** der potentielle Sender einer Nachricht oder von Daten und das Steuergerät **24** ist der potentielle Empfänger. Vor der tatsächlichen Übersendung einer Nachricht von dem Switch **36** zu dem Steuergerät **24** stellt sich allerdings die Frage, ob das Steuergerät **24** authentisch ist. Dies kann der Sender, das heißt der Switch **36** nicht wissen. Bevor eine Nachricht oder Daten gewissermaßen blind an das Steuergerät **24** geschickt werden, wird hier die Authentizität von Steuergerät **24** geprüft.

[0033] Dazu senden die Empfänger der entsprechenden Inhalte, hier das Steuergerät **24**, regelmäßige Authentizitätsbotschaften **44**, die sowohl vom zentralen Gateway beziehungsweise Busmaster **16** als auch von den möglichen Sendern, hier der Switch **36**, an diese Steuergeräte empfangen und validiert werden. Die Authentizitätsbotschaft **44** kann zyklisch oder auf Anfrage gesendet werden und enthält ein Authentizitätsmerkmal, wie eine Signatur. Die Signatur basiert auf dem symmetrischen Schlüssel **42**, wenn dieser zum Einsatz gelangt. Alternativ kann zum Beispiel eine konstante Zahl verwendet werden. Zusammengefasst sendet der Empfänger, das heißt hier das Steuergerät **24**, zyklische, signierte Authentizitätsbotschaften **44** mittels eines Vernetzungsbusunabhängigen Signaturprotokolls. Diese Nachrichten haben keinen applikativen Inhalt; sie bestehen nur aus der Signatur und gegebenenfalls einem Protokolloverhead.

[0034] Je nach verwendeter Netzinfrastruktur kann der Switch **36** die Authentizitätsbotschaft **44** direkt empfangen oder die Authentizitätsbotschaft **44** wird dem Switch **36** mittels des Busmasters **16** zugestellt. In diesem Fall wird zum Beispiel der Sender der eigentlichen applikativen Botschaft, das heißt der Switch **36**, über die Datenfestlegung als Empfänger der Authentizitätsbotschaft **44** festgelegt. Daraufhin kann der Busmaster **16** die Authentizitätsbotschaft **44** von dem Empfänger **24** an den Sender **36** weiterleiten. Generell werden die Authentizitätsbotschaften **44** zu jedem Sender mit Authentifizierungsbedarf dieses Empfängers weitergeleitet.

[0035] Nach erhaltener Authentizitätsbotschaft **44** führt der Switch **36** einen Authentifizierungsalgorithmus auf die Authentizitätsboschaft **44** beziehungsweise das Authentizitätsmerkmal aus und entscheidet oder prüft den Status der Authentizität, also der Integrität, von dem Empfänger **24**.

[0036] Falls die Authentifizierung erfolgreich ist, sendet der Sender, das heißt der Switch **36**, die Nachricht mit applikativem Inhalt beziehungsweise einer Nutzlast an den Empfänger, das heißt das Steuergerät **24**. Falls die Authentifizierung fehlschlägt, kann der Switch **36** geeignete, vorher definierte Ersatzreaktionen einleiten, wie zum Beispiel eine entsprechende Meldung an den Busmaster **16**. Somit ist die die Möglichkeit der Identifizierung nicht authentischer Empfänger gegeben.

[0037] **Fig.** 2 zeigt ein weiteres Ausführungsbeispiel einer Vorrichtung **100** zur Empfängerauthentifikation in einem Fahrzeug **120**. Die Vorrichtung **100** dient zur Authentifizierung von Empfängern in einem Netzwerk **140** des Fahrzeugs **120**. Das Fahrzeug **120** kann zum Beispiel ein PKW, LKW, Motorrad, Bus oder Bahn, sein. Als Fahrzeug werden hier sämtliche Land-, Luft- und Wasserfahrzeuge angesehen.

[0038] Das Netzwerk **140** hat einen Gateway oder Busmaster **160** für eine Netztopographie **180**. Zur Kommunikation mit der Netztopographie **180** hat der Busmaster **160** eine Netz-Schnittstelle **200**, zum Beispiel in Form eines Switches, Routers oder Hubs. Die Netz-Schnittstelle **200** kontrolliert die Netztopographie **180**, zum Beispiel in Form eines DNS-Servers

(Domain Name System). Die Netztopographie **180** kann zum Beispiel auf dem Ethernet-Standard basieren. An die Netz-Schnittstelle **200** sind direkt zwei Steuergeräte **220** und **240** angeschlossen. Die hier gezeigte Netzstruktur der Netztopographie **180** ist lediglich beispielhaft und kann alle technisch möglichen Kombinationen von Netzwerkkomponenten umfassen.

[0039] Die Teilnehmer des Netzwerks **140**, das heißt die Steuergeräte **220** und **240** und der Busmaster **160** kommunizieren miteinander. Diese Kommunikation kann zum Beispiel eine symmetrische Verschlüsselung verwenden. Dazu ist in jedem Teilnehmer mindestens ein symmetrischer Schlüssel **42** vorhanden, von denen der Übersicht wegen nur zwei in dem Steuergerät **240** und dem Busmaster **160** dargestellt sind. Diese in diesem Beispiel bereits vorhandenen symmetrischen Schlüssel **42** werden außerdem zur Prüfung der Authentizität von Steuergeräten verwendet, wie im Folgenden erläutert wird. Die Teilnehmer beziehungsweise die Steuergeräte **220** und **240** und der Busmaster **160** haben einen Authentifizierungsmechanismus für Nachrichten, mit dem sie in Kombination mit dem symmetrischen Schlüsselmaterial die Authentizität der Sender von Nachrichten überprüfen können.

[0040] In diesem Beispiel ist der Busmaster **160** beziehungsweise ein weiterer nicht dargestellter Teilnehmer wie ein Steuergerät der potentielle Sender einer Nachricht oder von Daten und das Steuergerät **240** ist der potentielle Empfänger. Es stellt sich allerdings die Frage, ob das Steuergerät **240** authentisch ist.

[0041] Der Busmaster **160** kann eine Soll-Liste aller Teilnehmer des Netzwerks **140** enthalten. Es kann vorgesehen sein, dass jeder Teilnehmer oder Slave, hier die beiden Steuergeräte **220** und **240** per Voreinstellung authentisch ist. Für einen aktuellen Abgleich senden die Teilnehmer, in diesem Beispiel das Steuergerät **240** Authentizitätsbotschaften **280**, die von dem zentralen Gateway beziehungsweise Busmaster **160** empfangen und validiert werden. Die Authentizitätsbotschaft **280** kann zyklisch oder auf Anfrage gesendet werden und enthält ein Authentizitätsmerkmal, wie eine Signatur. Die Signatur basiert auf dem symmetrischen Schlüssel **260**, wenn dieser zum Einsatz gelangt. Alternativ kann zum Beispiel eine konstante Zahl verwendet werden. Zusammengefasst sendet der Empfänger, das heißt hier das Steuergerät **240**, zyklische, signierte Authentizitätsbotschaften **280** mittels eines Vernetzungsbus-unabhängigen Signaturprotokolls. Diese Nachrichten haben keinen applikativen Inhalt; sie bestehen nur aus der Signatur und gegebenenfalls einem Protokolloverhead.

[0042] Der Busmaster **160**, der auch als Domänenmaster bezeichnet werden kann, kann diese Authentizitätsbotschaften **280** authentifizieren. Bei erfolgreicher Authentifizierung kann dies gegebenenfalls in der Soll-Liste aller Teilnehmer des Netzwerks **140** vermerkt werden und der Betrieb kann normal weiter laufen. Wenn die Authentifizierung fehlschlägt, kann zum Beispiel über einen Eintrag in der Soll-Liste eine Kennzeichnung für Aftersales Services, wie zum Beispiel für eine Kundendienstwerkstatt, zur Überprüfung und/oder Austausch vorgenommen werden. Es kann vorgesehen sein, dass der Busmaster **160** nur Teilnehmer auf Authentizität überprüft, die in der Soll-Liste aller Teilnehmer des Netzwerks **140** beziehungsweise in der Soll-Liste der dem Busmaster **160** zugeordneten Teilnehmer aufgeführt sind.

[0043] Mit diesem Vorgehen kann ein manipuliertes beziehungsweise getauschtes Steuergerät, das gemäß der Soll-Liste dem Busmaster **160** zugeordnet ist, in diesem Falle im Busmaster **160** als nicht authentischer Teilnehmer gekennzeichnet werden.

[0044] Somit ist die die Möglichkeit der Identifizierung nicht authentischer Empfänger gegeben.

Bezugszeichenliste

10	Vorrichtung
12	Fahrzeug
14	Netzwerk
16	Busmaster
18	Bussystem
20	Netztopographie
22	Bus-Schnittstelle
24	Steuergerät
26	Steuergerät
28	Steuergerät
30	Netz-Schnittstelle
32	Steuergerät
34	Steuergerät
36	Switch
38	Steuergerät
40	Steuergerät
42	symmetrischer Schlüssel
44	Authentizitätsbotschaft
100	Vorrichtung
120	Fahrzeug
140	Netzwerk
160	Busmaster
180	Netztopographie
200	Bus-Schnittstelle
220	Steuergerät
240	Steuergerät
260	symmetrischer Schlüssel
280	Authentizitätsbotschaft

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- WO 2005/115809 A1 [0004]
- WO 2005/116834 A1 [0005]

Patentansprüche

1. Verfahren zur Empfängerauthentifikation in einem Fahrzeugnetzwerk (**14**; **140**) mit mindestens einem Sender (**36**; **160**) und mindestens einem Empfänger (**24**; **240**), mit den Schritten:
– Senden eines Authentizitätsmerkmals durch den Empfänger (**24**; **240**);
– Empfangen des Authentizitätsmerkmals durch den Sender (**36**; **160**); und
– Prüfen der Authentizität des Empfängers (**24**; **240**) anhand des Authentizitätsmerkmals durch den Sender (**36**; **160**).

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,** dass das Authentizitätsmerkmal eine Signatur ist.

3. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** dass das Authentizitätsmerkmal auf zuvor in den mindestens einen Sender (**36**; **160**) und den mindestens einen Empfänger (**24**; **240**) symmetrischen Schlüsseln (**42**; **360**) basiert.

4. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** dass das Authentizitätsmerkmal zyklisch gesendet wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** dass das Authentizitätsmerkmal auf Anfrage gesendet wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** dass der mindestens eine Sender (**36**; **160**) und der mindestens eine Empfänger (**24**) Steuergeräte sind.

7. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** dass eine Nachricht durch den Sender (**36**; **160**) an den Empfänger (**24**; **240**) nur bei erfolgter Authentifizierung gesendet wird.

8. Vorrichtung zur Empfängerauthentifikation in einem Fahrzeugnetzwerk (**14**; **140**) mit mindestens einem Sender (**36**; **160**) und mindestens einem Empfänger (**24**; **240**), **dadurch gekennzeichnet,** dass der mindestens eine Empfänger (**24**; **240**) eingerichtet ist, ein Authentizitätsmerkmal zu senden und dass der mindestens eine Sender (**36**; **160**) eingerichtet ist, die Authentizität des Empfängers (**24**; **240**) anhand des Authentizitätsmerkmals zu prüfen.

9. Vorrichtung nach Anspruch 8, **dadurch gekennzeichnet,** dass der mindestens eine Sender (**36**) und der mindestens eine Empfänger (**24**) Steuergeräte sind.

10. Vorrichtung nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** dass der mindestens eine Sender (**160**) ein Busmaster des Fahrzeugnetzwerkes (**140**) ist.

11. Vorrichtung nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** dass der mindestens eine Sender (**36**; **160**) eingerichtet ist, bei erfolgreicher Prüfung eine Nachricht an den mindestens einen Empfänger (**24**; **240**) zu senden.

12. Fahrzeug mit einem Fahrzeugnetzwerk mit mindestens einem Sender (**36**; **160**) und mindestens einem Empfänger (**24**; **240**), **dadurch gekennzeichnet,** dass eine Vorrichtung (**10**; **100**) nach einem der Ansprüche 8 bis 11 vorgesehen ist.

Es folgt eine Seite Zeichnungen

Anhängende Zeichnungen

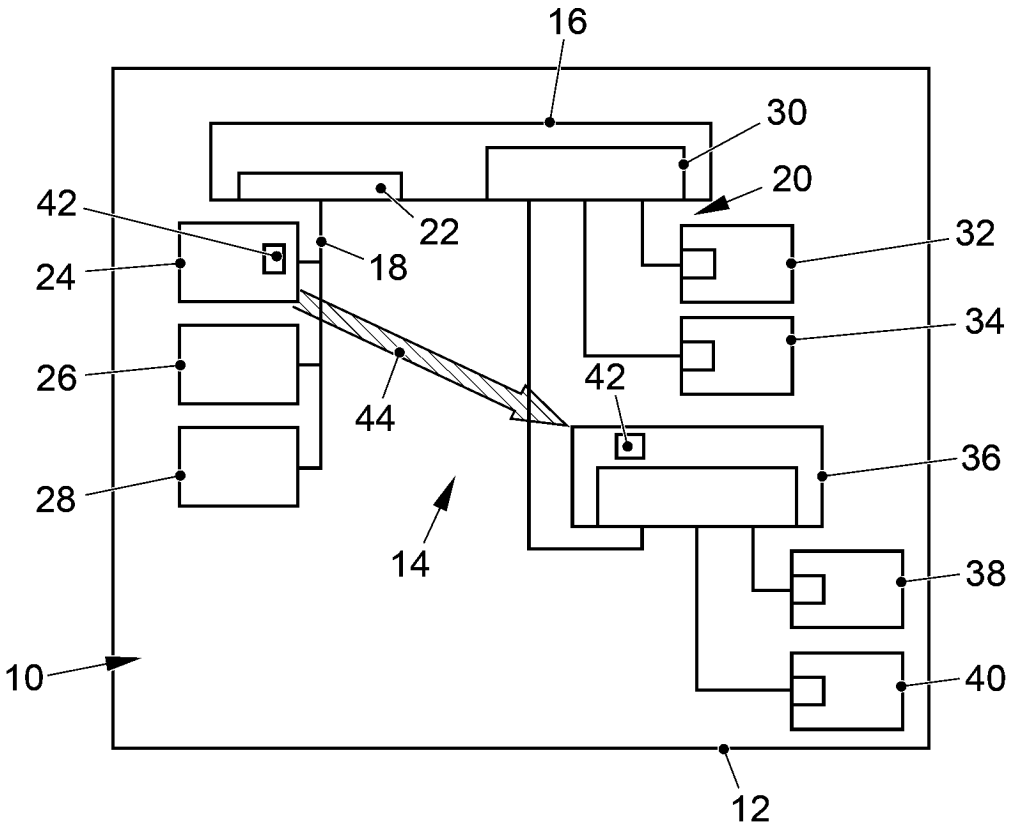


FIG. 1

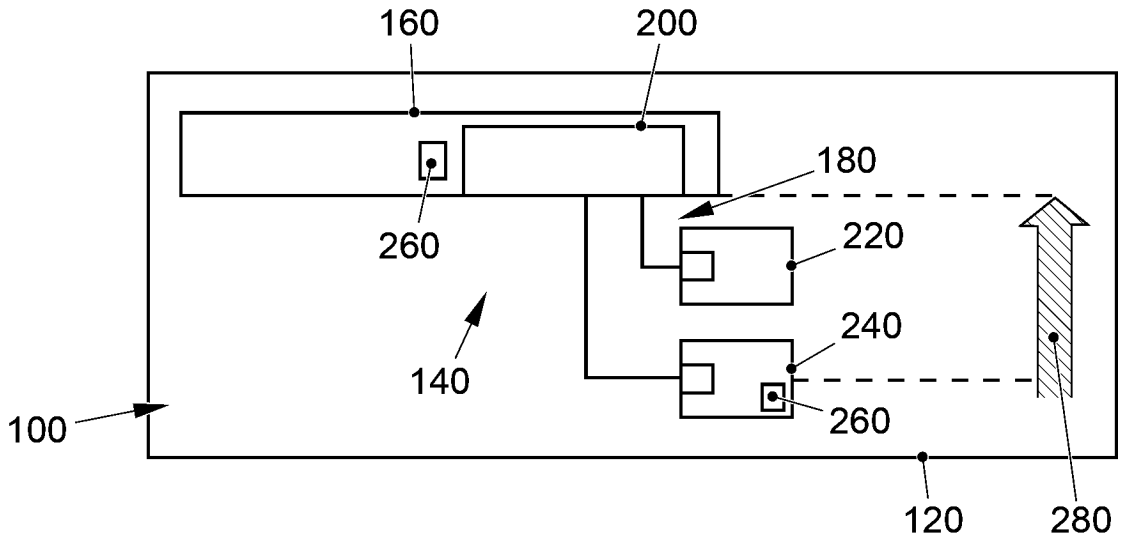


FIG. 2