(19) Deutsches Patent- und Markenamt

(10) **DE 10 2016 222 599 A1** 2018.05.17

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2016 222 599.5**
(22) Anmeldetag: **16.11.2016**
(43) Offenlegungstag: **17.05.2018**

(51) Int Cl.: ***H03M 13/09*** (2006.01)
H04L 9/32 (2006.01)

(71) Anmelder:
Continental Teves AG & Co. OHG, 60488 Frankfurt, DE

(72) Erfinder:
Muhm, Christian, 60487 Frankfurt, DE; Schreiner, Frank, Dr., 61381 Friedrichsdorf, DE

(56) Ermittelter Stand der Technik:

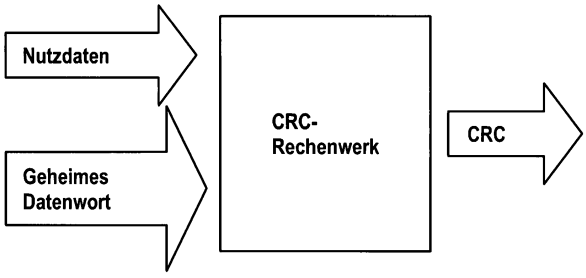
US	**7 457 410**	**B2**

Rechercheantrag gemäß § 43 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Verfahren zur Absicherung der Datenübertragung in einem Datenbus**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Absicherung der Datenübertragung in einem Datenbus, über den Datenprotokolle von mindestens einem Sender an wenigstens einen Empfänger übermittelt werden, wobei die Datenprotokolle zur Übermittlung von physikalisch übertragbaren Nutzdaten und einer CRC-Prüfsumme ein Datenfeld mit vorgegebener Länge enthalten. Erfindungsgemäß ist vorgesehen, dass wenigstens ein geheimes Datenwort in dem Sender und dem Empfänger bereitgestellt wird und die CRC-Prüfsumme aus den zu übertragenden Nutzdaten und dem geheimen Datenwort berechnet wird.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Absicherung der Datenübertragung in einem Datenbus, über den Datenprotokolle mindestens eines Senders an wenigstens einen Empfänger weitergegeben werden, die mindestens ein Datenfeld mit vorgegebener Länge und ein Sicherungsfeld mit einer CRC-Prüfsumme enthalten.

[0002] Für die Kommunikation zwischen Steuergeräten in einem Fahrzeug sind verschiedene Bussysteme bekannt, wie bspw. der bekannte CAN-Bus (Controller Area Network). Daneben gibt es aber auch andere Bussysteme, die ebenfalls im Automobilbau Anwendung finden, wie LIN (Local Interconnect Network), FlexRay, MOST (Media Oriented Systems Transport), PSI5 (Peripheral Sensor Interface 5), sowie das aus dem Computerbereich bekannte Ethernet.

[0003] Über ein CAN-Netzwerk werden die zwischen Steuergeräten im Fahrzeug ausgetauschten Informationen in Datentelegrammen bzw. Botschaften, sogenannten CAN-Frames, im Folgenden auch Datenprotokolle genannt, zusammengefasst. Ein solches Datenprotokoll ist in bekannter Weise aus folgenden Feldern zusammengesetzt: Einem Anfangsfeld (Start of Frame), einem Arbitrations-Feld (Arbitration Field), einem Kontrollfeld (Control Field), einem Datenfeld (Data Field), einem Sicherungsfeld (CRC Field), einem Bestätigungsfeld (ACK Field), einem Endfeld (End of Frame) und einem Ruhezustands-Feld (Inter Frame Space).

[0004] Dieses CAN-Datenprotokoll enthält die an den jeweiligen Busteilnehmer zu übertragende Information im Datenfeld (Data Field), das heißt die Nutzdaten, die in Form einer Bitfolge mit einer fest vorgegebenen Bitanzahl vorliegen. Ein CAN-Frame kann dabei bis zu 64 Bit an Nutzdaten übertragen. Diese Daten können sicherheitsrelevante Steuerbefehle oder Zustandsdaten enthalten. Falsch gesendete, falsch übertragene oder falsch empfangene Daten können in modernen Fahrzeugen zu Gefahren für die Gesundheit und das Leben der Fahrzeuginsassen oder anderer Verkehrsteilnehmer führen.

[0005] Die Absicherung der Datenkommunikation wird im Rahmen der standardisierten Softwarearchitektur AUTOSAR® (AUTomotive Open System ARchitecture) zwischen den Software-Komponenten durch einen softwarebasierten E2E(End-to-End)-Schutzmechanismus realisiert. Hierbei werden mittels Prüfsummen (CRC) und Botschaftszählern Übertragungsfehler erkannt (vgl. Specification of SW-C End-to-End Communication Protection Library AUTOSAR Release 4.2.2).

[0006] Um gemäß diesem E2E-Schutzmechanismus die zu übertragenden Nutzdaten, bspw. über einen CAN-Bus gegen zufällige Übertragungsfehler abzusichern, werden Prüfdaten in dem Datenfeld mitgesendet, die eine Verfälschung der Daten erkennen lassen. Üblicherweise werden dafür - wie oben ausgeführt - CRC-Prüfsummen und Botschaftszähler eingesetzt, die vom sendenden Steuergerät in den 64 Bit des Datenfeldes der CAN-Botschaft mitgesendet werden. Das Datenfeld eines solchen Datenprotokolls zeigt **Fig. 2**, welches aus N 8-Bit-Datenfeldabschnitten aufgebaut ist. Der erste Datenfeldabschnitt Data [0] enthält eine 8-Bit-CRC-Prüfsumme, während die verbleibenden Datenfeldabschnitte Data [1] bis Data [N] die physikalisch übertragbaren Nutzdaten enthalten. Gemäß der oben genannten AUTOSAR-Spezifikation enthält der zweite Datenfeldabschnitt Data [1] den Stand des Botschaftszählers - oft bestehend aus 4 Bit - und 4 Bit Nutzdaten. Bei der Verwendung des CAN-Busses als Kommunikationsmittel zwischen den Steuergeräten eines Fahrzeugs ist N=8, d. h. die Länge des Datenfeldes beträgt 64 Bit. Wird eine 8-Bit-CRC-Prüfsumme zusammen mit den Nutzdaten in einem solchen Datenfeld übertragen, kann die maximale Länge der zu übertragenden Nutzdaten 56 Bit betragen. Wird zusätzlich noch der Stand des Botschaftszählers übertragen, verbleiben 52 Bit für die Nutzdaten.

[0007] Nach der Übermittlung eines solchen Datenfeldes gemäß **Fig. 2** prüft der empfangende Busteilnehmer die Korrektheit der Datenübertragung, indem er aus den gesendeten Daten und gegebenenfalls weiteren Zusatzinformationen selbst eine CRC-Prüfsumme berechnet und diese mit der CRC-Prüfsumme im empfangenen Datenprotokoll vergleicht. Stimmt die berechnete CRC-Prüfsumme mit der im Datenprotokoll übertragenen CRC-Prüfsumme überein, liegt eine fehlerfreie Datenübertragung vor.

[0008] Diese CRC-Prüfsummen und Botschaftszähler sind ausreichend geeignet, um zufällige Verfälschungen aufgrund von physikalischen Einflüssen (z.B. Hardware-Fehler oder Störeinstrahlung) im empfangenden Steuergerät zu erkennen.

[0009] Die Datenprotokolle inklusive der Prüfdaten sind bei dem bekannten CAN-Bus nicht gegen böswillige Manipulation abgesichert. Ein Angreifer, der Zugang zum CAN-Bus eines Fahrzeugs gefunden hat, kann CAN-Botschaften mit korrekt errechneten Prüfdaten verschicken. Diese Botschaften werden von den anderen Steu-

ergeräten im Fahrzeug als gültig angesehen. Somit kann ein Angreifer mit Zugriff auf das CAN-Netzwerk auch Botschaften senden, die das Leben der Fahrzeuginsassen gefährden.

[0010] Hinsichtlich dieses Problems schlägt bspw. die DE 10 2012 210 327 A1 ein Verfahren zum Übertragen von Nachrichten in einem Fahrzeug-Kommunikationssystem vor, mit welchem eine Manipulation oder Veränderung einer über einen Datenbus übertragenen Nachricht von einem Sender an einen Empfänger erkannt werden kann. Hierzu wird für die zu übermittelnde Nachricht eine Signatur ermittelt und zusammen als Signatur-Nachricht vom Empfänger empfangen. Die Überprüfung der Signatur durch den Empfänger erfolgt durch erneutes Ermitteln der Signatur für die übertragene Nachricht und deren Vergleich mit der in der Signatur-Nachricht enthaltenen Signatur.

[0011] Die Signatur gemäß dieser DE 10 2012 210 327 A1 wird aus der zu schützenden Nachricht, aus einem ersten Zähler und aus einem zweiten Zähler unter Verwendung eines dem Sender und den Empfänger bekannten und geheimen Schlüssels erzeugt. Eine Manipulation oder Veränderung einer übertragenen Nachricht kann bspw. dadurch erkannt werden, wenn die zu schützende Nachricht parallel zu der Signatur-Nachricht in einer weiteren, jedoch nicht signierten Nachricht von dem Sender an den Empfänger übertragen wird. In der nichtsignierten Nachricht wird die zu schützende Nachricht im Klartext übertragen. Die Berechnung der Signatur über die im Klartext übertragene Nachricht führt dann zu einer anderen Signatur, wenn davon ausgegangen wird, dass die mit der Signatur-Nachricht geschützte Nachricht nicht manipuliert ist.

[0012] Damit gemäß dieser DE 10 2012 210 327 A1 der Empfänger zur Überprüfung der Signatur den hierfür benötigten Wert des ersten Zählers verarbeiten kann, wird dieser dem Empfänger über eine separate Nachricht mitgeteilt. Der Wert des zweiten Zählers wird mit jeder übertragenen Signatur-Nachricht in vorgegebener Weise verändert und mit der zu schützenden Nachricht an den Empfänger als Signatur-Nachricht übertragen.

[0013] Wird dieses bekannte Verfahren gemäß der DE 10 2012 210 327 A1 bei einem CAN-Bus angewendet, wird nur ein Teil der Signatur im Datenfeld zusammen mit den Nutzdaten übertragen, da die vollständige Signatur in Abhängigkeit des verwendeten Algorithmus 128 Bit oder länger oder kürzer sein kann, jedoch das Datenfeld einer CAN-Botschaft lediglich 64 Bit lang ist.

[0014] Der Nachteil dieses bekannten Verfahrens gemäß der DE 10 2012 210 327 A1 besteht darin, dass das Datenfeld zur Übertragung einer Signatur verwendet wird und daher dieses Datenfeld nicht vollständig zur Übertragung von Nachrichten zur Verfügung steht.

[0015] Des Weiteren beschreibt die DE 10 2010 033 229 A1 ein Verfahren zur manipulationssicheren Übertragung von Steuerdaten zwischen Steuereinheiten eines Netzwerks. Bei diesem Verfahren werden senderseitig Integritätsprüfinformationsdaten für die von einer ersten Steuereinheit gesendeten Steuerdaten erzeugt, eine kryptographische Prüfsumme für die senderseitig erzeugten Integritätsprüfinformationsdaten mittels eines kryptographischen Schlüssels berechnet, die senderseitig erzeugten Integritätsprüfinformationsdaten und die berechnete kryptographischen Prüfsumme zu einer Integritätsprüfverifikationseinheit übermittelt, welche die kryptographische Prüfsumme mittels eines kryptographischen Schlüssels empfangsseitig verifiziert, empfangsseitig Integritätsprüfinformationsdaten für die durch eine zweite Steuereinheit empfangenen Steuerdaten erzeugt und die empfangsseitig erzeugten Integritätsprüfinformationsdaten mit den zusammen mit der verifizierten kryptographischen Prüfsumme empfangenen senderseitig erzeugten Integritätsprüfinformationsdaten zur Erkennung einer Manipulation der übertragenen Steuerdaten verglichen. Die senderseitig erzeugten Integritätsprüfinformationsdaten werden durch einen Hash-Wert von einem Teil der in einem Steuerdatenpaket oder in einer bestimmten Anzahl von Steuerdatenpaketen enthaltenen Steuerdaten gebildet. Die Steuerdaten werden bei diesem bekannten Verfahren unverschlüsselt entweder zeitversetzt zu den Integritätsprüfinformationsdaten mit zugehörigen kryptographischen Prüfsumme oder zusammen mit denselben übertragen.

[0016] Dieses bekannte Verfahren gemäß der DE 10 2010 033 229 A1 ist wohl in einfacher Weise implementierbar und in einem Kommunikationssystem nachrüstbar, jedoch erfordert deren Realisierung einen hohen hardwaremäßigen Aufwand, da zur Erzeugung der Integritätsprüfinformationsdaten senderseitig eine Integritätsprüferzeugungseinheit und empfangsseitig eine Integritätsprüfverifikationseinheit erforderlich sind.

[0017] Schließlich ist auch aus der DE 10 2008 046 563 A1 ein Verfahren zur kryptografisch geschützten Übertragung von Daten zwischen Netzwerkknoten eines Netzwerks bekannt. Um mit diesem bekannten Verfahren „Replay-Attacken“ zu verhindern, werden NONCE-Werte eingesetzt. Ein NONCE-Wert stellt einen Einmal-Wert bzw. einen nur einmalig zu verwendenden Wert dar. Der NONCE-Wert dient zur Erkennung von wieder eingespielten Nachrichten (Replay-Attacken). Die Verschlüsselung der Nutzdaten seitens eines Sen-

deknotens erfolgt dann in Abhängigkeit von einem Schlüssel und einem NONCE-Wert. Bei diesem bekannten Verfahren werden zur Übertragung der Daten in einer Nachricht die folgenden Schritte ausgeführt: Bilden eines NONCE-Wertes aus einem Zählwert, welcher bei der Übertragung der Nachricht aktualisiert wird, und aus einem Konstantwert, welcher den Netzwerkknoten des Netzwerkes gemeinsam zur Verfügung gestellt wird, und Ver- und Entschlüsseln der in der Nachricht übertragenen Daten mittels eines kryptographischen Schlüssels und des gebildeten NONCE-Wertes.

[0018] Das Datenprotokoll zur Übertragung von Nutzdaten umfasst Header-Daten, welche eine Sendeknotenadresse, eine Empfangsknotenadresse und den aktuellen Zählwert des sendenden Netzwerkknotens umfassen. Empfangsseitig vergleicht der Empfangsnetzwerkknoten den in der Nachricht übertragenen Zählwert des Sendenetzwerkknotens mit einem anhand der in der Nachricht übertragenen Sendeknotenadresse selektierten Zählwert eines internen Zählers des Empfangsnetzwerkknotens und bildet aus dem übertragenen Zählwert, aus dem gemeinsamen Konstantwert und aus der übertragenen Sendeknotenadresse einen empfangsseitigen NONCE-Wert, falls der übertragene Zählwert aktueller ist als der selektierte Zählwert, wobei der empfangsseitig gebildete NONCE-Wert und ein in dem Empfangsnetzwerkknoten gespeicherter Schlüssel zur Entschlüsselung der in der Nachricht verschlüsselt übertragenen Daten benutzt werden.

[0019] Dieses bekannte Verfahren gemäß der DE 10 2008 046 563 A1 erfordert zu dessen Realisierung einen hohen Rechenaufwand, da nicht nur die NONCE-Werte berechnet werden müssen, sondern auch die Nutzdaten mittels eines Schlüssels verschlüsselt werden müssen.

[0020] Der Vollständigkeit halber sei noch auf die US 2002/0174332 A1 verwiesen, welche den Message Authentication Code (MAC) zur Prüfung der Integrität von zwischen einem Sender und einem Empfänger übermittelten Daten oder Nachrichten verwendet. Ein MAC-Algorithmus erfordert zwei Eingabeparameter, zum einen die zu schützenden Nachrichten und zum anderen einen geheimen Schlüssel. Aus beidem wird mittels des MAC-Algorithmus eine Prüf summe, der Message Authentication Code berechnet. Ein Sender berechnet mittels des Schlüssels und der zu übertragenden Nachricht die MAC-Prüfsumme und sendet dann die unverschlüsselte Nachricht und die MAC-Prüfsumme an einen Empfänger. Dieser berechnet die MAC-Prüfsumme aus der empfangenen Nachricht mit dem Schlüssel und vergleicht die berechnete MAC-Prüfsumme mit der empfangenen. Die Nachricht wird nur akzeptiert, wenn beide Werte übereinstimmen.

[0021] Mit dem Verfahren zur Prüfung der Integrität von Nachrichten zwischen einer mobilen Station und einem Mobilfunknetz gemäß dieser US 2002/0174332 A1 ist es möglich, die MAC-Prüfsumme gekürzt zu übertragen, wenn die Länge aus zu übertragenden Nachricht und der ungekürzten MAC-Prüfsumme zu lang ist, also länger ist als das Datenfeld des Datenprotokolls.

[0022] Die Aufgabe der Erfindung besteht darin, ein Verfahren zur Absicherung der Datenübertragung in einem Datenbus eines Fahrzeugs anzugeben, welches die Datenübertragung in dem Datenbus, insbesondere in einem CAN-Bus widerstandsfähiger gegen Hackerangriffe macht und mit geringem Aufwand realisierbar ist.

[0023] Die Aufgabe wird gelöst durch ein Verfahren mit den Merkmalen des Patentanspruchs 1.

[0024] Bei diesem Verfahren zur Absicherung der Datenübertragung in einem Datenbus, über den Datenprotokolle von mindestens einem Sender an wenigstens einen Empfänger übermittelt werden, wobei die Datenprotokolle zur Übermittlung von physikalischen übertragbaren Nutzdaten und einer CRC-Prüfsumme ein Datenfeld mit vorgegebener Länge enthalten, ist erfindungsgemäß vorgesehen, dass

- wenigstens ein geheimes Datenwort in dem Sender und dem Empfänger bereitgestellt wird, und
- die CRC-Prüfsumme aus den zu übertragenden Nutzdaten und dem geheimen Datenwort berechnet wird.

[0025] Bei diesem erfindungsgemäßen Verfahren wird das geheime Datenwort lediglich dazu benutzt, zusammen mit den Nutzdaten des Datenfeldes eine CRC-Prüfsumme zu bilden, die einschließlich der Nutzdaten in dem Datenfeld übertragen wird. Eine solche CRC-Prüfsumme unterscheidet sich von derjenigen, die ohne ein solches geheimes Datenwort berechnet wird.

[0026] Unter physikalisch übertragbaren Nutzdaten werden solche als bitserielle Datenströme vorliegenden Nutzdaten bezeichnet, welche von einem Datenbus, bspw. dem CAN-Bus als Übertragungsmedium in die entsprechenden BUS-Signale umsetzbar sind.

[0027] Nach einer vorteilhaften Weiterbildung des erfindungsgemäßen Verfahrens wird das geheime Datenwort mit einer Länge bereitgestellt, die größer ist als die Länge der CRC-Prüf-summe. Wird bspw. eine 8-Bit-CRC verwendet, ist die Länge des geheimen Datenwortes länger als 8 Bit, also bspw. ein Vielfaches von 1 Byte. Die Länge eines solchen geheimen Datenwortes kann dann bspw. 64 oder 128 Bit usw. sein.

[0028] Durch die gegenüber der CRC-Prüfsumme größere Länge des geheimen Datenwortes wird bewirkt, dass das geheime Datenwort von einem böswilligen Angreifer sehr viel schwerer erraten werden kann. Bei einer Länge des geheimen Datenwortes von bspw. 64 Bit beträgt die Chance des Erratens 1:2^64, also 1: 18.446.744.073.709.551.616. In der Praxis ist somit ein Erraten des geheimen Datenwortes für einen böswilligen Angreifer nicht mehr durchführbar.

[0029] Da bei dem Empfänger das gleiche geheime Datenwort zur Verfügung steht, kann empfängerseitig aus den Nutzdaten zusammen mit dem geheimen Datenwort die CRC-Prüfsumme berechnet und mit der empfangenen CRC-Prüfsumme verglichen werden. Wenn die derart vorliegenden CRC-Prüfsummen nicht übereinstimmen, wird das übermittelte Datenprotokoll und damit auch die empfangenen Nutzdaten verworfen.

[0030] Bei Verwendung dieses erfindungsgemäßen Verfahrens müssen die in dem Datenbus bereits definierten und implementierten Sicherheitskonzepte und Fehlerreaktionen auf falsche Nutzdaten nicht verändert werden. Dies gilt insbesondere, wenn der Datenbus als CAN-Bus ausgebildet ist. Auch müssen bei einem solchen CAN-Bus die sicherheitsrelevanten CAN-Datenproto-kolle nicht angepasst werden, wenn bereits ausreichende CRC-Prüfsummen mit ausreichender Lücke für ein geheimes Datenwort eingesetzt werden. Schließlich erfordert der Einsatz dieses erfindungsgemäßen Verfahrens auf der Ebene des mit dem Datenbus realisierten Netzwerkes keine zusätzliche Hardware, um mit diesem erfindungsgemäßen Verfahren dieses Netzwerk gegen Hackerangriffe zu schützen.

[0031] Es ist nach einer weiteren bevorzugten Weiterbildung der Erfindung auch möglich, das geheime Datenwort mittels eines kryptographischen Verfahrens in Speichereinheiten des Senders und des Empfängers zu speichern. Hierfür können gehärtete Krypto-Speicher sowohl für den Sender als auch für den Empfänger eingesetzt werden. Bei Verwendung des geheimen Datenwortes werden abgesicherte Krypto-Algorithmen und Krypto-Hardware, wie bspw. ein Hardware-Sicherheitsmodul (Hardware Security Module) eingesetzt. Ein solches Hardware-Sicherheitsmodul ist eine Komponente für die effiziente und sichere Ausführung von kryptographischen Operationen oder Applikationen, wie bspw. die Erzeugung von kryptographischen Schlüsseln, um die Vertrauenswürdigkeit und die Integrität von Daten sicherzustellen. Mit einem solchen Hardware-Sicherheitsmodul ist es daher auch möglich das geheime Datenwort gemäß des erfindungsgemäßen Verfahrens zu erzeugen oder dieses zu speichern, um es vor unberechtigtem Zugriff zu schützen.

[0032] Nach einer weiteren bevorzugten Ausgestaltung der Erfindung wird das geheime Datenwort nach einer vorgegebenen Anzahl von versendeten Datenprotokollen gegen ein anderes geheimes Datenwort ausgetauscht. Insbesondere ist es damit möglich, nach jeder versendeten Nachricht ein Wechsel des geheimen Datenwortes vorzunehmen, d. h. jedes geheime Datenwort wird nur einmalig verwendet.

[0033] Hierzu wird ein neues geheimes Datenwort mittels des Algorithmus erzeugt oder ein weiteres in dem gehärteten Krypto-Speicher abgelegtes Datenwort als neues geheimes Datenwort verwendet. Dies setzt natürlich voraus, dass in dem gehärteten Krypto-Speicher mehrerer solcher geheimen Datenwörter vorgehalten werden. Die Gültigkeitsdauer eines aktuellen geheimen Datenwortes ist auch dem Empfänger bekannt, so dass der senderseitige Wechsel des geheimen Datenwortes dem Empfänger nicht mitgeteilt zu werden braucht.

[0034] Der Austausch des geheimen Datenwortes erschwert Hackerangriffe, bei denen das geheime Datenwort durch Mithören und Analysieren des Datenverkehrs auf dem CAN-Bus errechnet wird oder bei denen das geheime Datenwort erraten oder ausprobiert wird.

[0035] Ein Austausch des geheimen Datenwortes kann gemäß einer weiteren Ausgestaltung des erfindungsgemäßen Verfahrens auch dann vorgenommen werden, wenn ein kryptografisch abgesichertes Datenprotokoll vom Sender an den Empfänger oder umgekehrt vom Empfänger an den Sender übertragen wurde. Bei einem kryptografisch abgesicherten Datenprotokoll werden die Nutzdaten in dem Datenfeld nicht unverschlüsselt, sondern mittels eines Schlüssels vor der Übertragung an den Empfänger verschlüsselt.

[0036] Eine weitere vorteilhafte Ausgestaltung der Erfindung sieht vor, dass nach einer vorgegebenen Folge von fehlerhaft von dem Empfänger empfangenen Prüfsummen das geheime Datenwort ausgetauscht wird und dem Sender vom Empfänger der Austausch des geheimen Datenwortes mitgeteilt wird. So kann bspw. bereits

nach einem einzigen fehlerhaft übermittelten Datenprotokoll das geheime Datenwort ausgetauscht werden. Es ist auch möglich, nach einer vorgegebenen Anzahl von direkt aufeinanderfolgenden oder nicht direkt aufeinanderfolgenden fehlerhaft übermittelten Datenprotokollen das geheime Datenwort auszutauschen.

[0037] Zudem ist es weiterbildungsgemäß vorgesehen, dass nach einer vorgegebenen Folge von fehlerhaft von dem Empfänger empfangenen Prüfsummen dieser Empfänger in einen Notbetrieb übergeht, in welchem keine Datenprotokolle von dem Empfänger akzeptiert werden. So kann bspw. bereits nach einem einzigen fehlerhaft übermittelten Datenprotokoll der Empfänger in den Notbetrieb übergehen. Es ist auch möglich, dass nach einer vorgegebenen Anzahl von direkt aufeinanderfolgenden oder nicht direkt aufeinanderfolgenden fehlerhaft übermittelten Datenprotokollen der Empfänger in den Notbetrieb übergeht.

[0038] Um den Austausch von geheimen Datenworten zu ermöglichen, werden diese in Speichereinheiten des Senders und des Empfängers abgelegt. Weiterbildungsgemäß ist es vorgesehen, dass die Abfolge der zum Austausch bereitgestellten geheimen Datenworte vorab festgelegt wird.

[0039] Das erfindungsgemäße Verfahren ist besonders zur Anwendung bei einem CAN-Bus als Übertragungsmedium zwischen Steuergeräten eines Fahrzeugs geeignet. Anwendbar ist es auch in Flexray-, CAN-FD-, LIN-, MOST- und Ethernet-Netzwerken.

[0040] Das erfindungsgemäße Verfahren wird nachfolgend anhand von Ausführungsbeispielen des erfindungsgemäßen Verfahrens unter Bezugnahme auf die beigefügten Figuren beschrieben und erläutert. Es zeigen:

Fig. 1 eine schematische Darstellung der erfindungsgemäßen Erzeugung einer CRC-Prüfsumme für die Übertragung eines CAN-Datentelegramms, und

Fig. 2 ein Datenfeld eines Datenprotokolls gemäß AUTOSAR®-Spezifikationen.

[0041] Das Datenfeld gemäß **Fig. 2** ist bereits in der Beschreibungseinleitung beschrieben. Daher wird lediglich gegebenenfalls im Zusammenhang mit der Beschreibung von **Fig. 1** hierauf verwiesen.

[0042] Die CRC-Prüfsumme, die mit einer CAN-Botschaft bzw. einem CAN-Datenprotokoll mitgesendet wird, dient wie eingangs bereits beschrieben der Fehlererkennung. Die CRC-Prüfsumme wird berechnet, indem die 0-1-Folge der zu übertragenden Nutzdaten des Datenfeldes als binäres Polynom interpretiert und durch ein ausgewähltes CRC-Polynom (Generator-Polynom) mod(2) dividiert wird, wobei der Rest der Division die CRC-Prüfsumme bildet.

[0043] Die Länge der CRC-Prüfsumme richtet sich nach der Anzahl der abzusichernden Nutzdatenbits der Nutzdaten und nach der benötigten Übertragungssicherheit, also der Hamming-Distanz. Eine große Anzahl von abzusichernden Datenbits erfordert bei gleicher Hamming-Distanz eine längere Prüfsumme. In der Regel richtet sich die Länge der Prüfsumme nach der maximal möglichen Anzahl von abzusichernden Datenbits.

[0044] Das Datenfeld gemäß **Fig. 2** enthält in dem Datenfeldabschnitt Data [0] eine 8-Bit-CRC-Prüfsumme, die mehr Bits absichern kann als es der Länge der Nutzdaten, also der Anzahl der Bits dieser Nutzdaten entspricht. In einem CAN-Datenprotokoll ist das Datenfeld **64** Bit lang, abzüglich der 8-Bit-CRC verbleibt für die zu übertragenden Nutzdaten eine Länge von 56 Bits, d.h. die CRC-Prüfsumme sichert eine größere Anzahl von Bits ab. Die Differenz zwischen der möglichen Anzahl der von der CRC-Prüfsumme abzusichernden Bits und der Länge der Nutzdaten wird benutzt, um ein geheimes Datenwort bei der Berechnung der CRC-Prüfsumme zu verwenden.

[0045] Wird bspw. das 8-Bit-CRC-Polynom ‘0x97:

$$(x+1) * \left(x\hat{}7 + x\hat{}6 + x\hat{}5 + x\hat{}2 + 1\right)$$

(entnommen aus ‚Philip Koopman, Tridib Chakravarty, DSN-**2004**: Cyclic Redundancy Code (CRC) Polynomial Selection For Embedded Networks‘) verwendet, können 119 Bits Nutzdaten mit einer Hamming-Distanz HD= 4 abgesichert werden.

[0046] Damit beträgt die Differenz zwischen der Anzahl der mit diesem CRC-Polynom ‘ 0x97 absicherbaren Bits (**119** Bits) und der Länge der abzusichernden Nutzdaten im CAN-Datenprotokoll (**56** Bits): 119-56 = 63 Bits. Folglich stehen für das geheime Datenwort **63** Bits zur Verfügung und es kann daher im vorliegenden Beispiel aus maximal 63 Bits bestehen. Werden andere CRC-Polynome oder andere Hamming-Distanzen für die CRC-Prüfsumme gewählt, kann das geheime Datenwort auch kürzer oder länger sein.

[0047] Zur Bestimmung der CRC-Prüfsumme wird das entsprechend den oben beschriebenen Methoden bereitgestellte geheime Datenwort, welches aus einer 0-1-Folge besteht, an die Nutzdaten angehängt und zusammen als Eingangsparameter einem CRC-Rechenwerk zugeführt, wie dies in **Fig. 1** schematisch dargestellt ist. Diese CRC-Prüfsumme zeigt natürlich einen anderen Wert, als eine lediglich aus den Nutzdaten des Datenfeldes berechnete CRC-Prüfsumme.

[0048] Diese derart aus den Nutzdaten und dem geheimen Datenwort berechnete CRC-Prüfsumme wird in dem Datenfeldabschnitt Data [0] nach **Fig. 2** eingetragen und zusammen mit den Nutzdaten des Datenfeldes von einem als Steuergerät ausgebildeten Sender eines CAN-Netzwerks einem ebenso als Steuergerät ausgebildeten Empfänger übermittelt.

[0049] Das geheime Datenwort ist nur dem Sender des CAN-Datenproto-kolls und dem Empfänger dieser CAN-Botschaft bekannt.

[0050] Die mit dem oben beschriebenen CRC-Polynom ‘0x97 berechnete Prüfsumme ist 1 Byte lang und weist eine ausreichend hohe Hamming-Distanz zur Absicherung von sicherheitsrelevanten Botschaften auf. Die Chance eine falsche Nachricht ohne Kenntnis des geheimen Datenwortes zu erzeugen, die vom Empfänger des CAN-Datenprotokolls als Botschaft akzeptiert wird, ist gleich 2^ (-Anzahl der CRC-Bits), dies entspricht 2^ (-8) = 1/256 = 0,39%.

[0051] Das in dem Sender als auch in dem Empfänger des CAN-Netz-werks bereitgestellte geheime Datenwort wird mittels eines vorgegebenen Algorithmus sowohl in dem Sender als auch in dem Empfänger erzeugt. Somit kann für jede Datenübertragung mittels des CAN-Datenprotokolls ein neues geheimes Datenwort verwendet werden, wodurch sich die Sicherheit der Datenübertragung verbessert, insbesondere Hackerangriffe erschwert werden.

[0052] Es ist auch möglich eine vorgegebene Anzahl von geheimen Datenworten jeweils in einer Speichereinheit des Senders und des Empfängers des CAN-Netzwerks bereitzustellen, um somit ggf. das geheime Datenwort zu wechseln.

[0053] Um ein solches in der Speichereinheit gespeicherte geheime Datenwort gegen Ausspähung zu sichern können folgende Maßnahmen realisiert werden:

- Verwendung von gehärteten Krypto-Speichern für das geheime Datenwort in den als Steuergeräte ausgebildeten Sendern und Empfängern des CAN-Netzwerks.

- Verwendung von abgesicherten Krypto-Algorithmen und Krypto-Hardware, bspw. Hardware-Sicherheitsmodulen (Hardware Security Module) bei Verwendung des geheimen Datenwortes.

- Einrichten von Schutzmaßnahmen vor Ausspähung des geheimen Datenwortes während des Entwicklungs-und Produktionsprozesses der als Sender und Empfänger eingesetzten Steuergeräte des CAN-Netzwerks.

[0054] Das geheime Datenwort kann auch nach einer vorgegebenen Anzahl von versendeten Datenprotokollen ausgetauscht werden, bspw. nach jeder versendeten Nachricht, d.h. jedes geheime Datenwort wird nur einmalig verwendet.

[0055] Ein Austausch des geheimen Datenwortes kann auch dann vorgenommen werden, wenn ein kryptografisch abgesichertes Datenprotokoll vom Sender an den Empfänger oder umgekehrt vom Empfänger an den Sender übertragen wurde. Bei einem kryptografisch abgesicherten Datenprotokoll werden die Nutzdaten in dem Datenfeld nicht unverschlüsselt, sondern mittels eines Schlüssels vor der Übertragung an den Empfänger verschlüsselt.

[0056] Ferner ist ein Austausch des geheimen Datenwortes nach einer vorgegebenen Folge von fehlerhaft von dem Empfänger empfangenen Prüfsummen durchführbar. In diesem Fall wird der Sender vom Empfänger über den Austausch des geheimen Datenwortes informiert. So kann bspw. bereits nach einem einzigen feh-

lerhaft übermittelten Datenprotokoll das geheime Datenwort ausgetauscht werden. Es ist auch möglich, nach einer vorgegebenen Anzahl von direkt aufeinanderfolgenden oder nicht direkt aufeinanderfolgenden fehlerhaft übermittelten Datenprotokollen das geheime Datenwort auszutauschen.

[0057] Zudem kann das CAN-Netzwerk so eingerichtet werden, dass nach einer vorgegebenen Folge von fehlerhaft von dem Empfänger empfangenen CRC-Prüfsummen dieser Empfänger in einen Notbetrieb übergeht, in welchem keine Datenprotokolle von dem Empfänger akzeptiert werden. So kann bspw. bereits nach einem einzigen fehlerhaft übermittelten Datenprotokoll der Empfänger in den Notbetrieb übergehen. Es ist auch möglich, dass nach einer vorgegebenen Anzahl von direkt aufeinanderfolgenden oder nicht direkt aufeinanderfolgenden fehlerhaft übermittelten Datenprotokollen der Empfänger in den Notbetrieb übergeht.

[0058] Die Abfolge der zu verwendenden geheimen Datenworte kann bereits vorab softwaremäßig in dem Sender und dem Empfänger festgelegt werden. Es ist auch möglich, dass die Abfolge der zum Austausch bereitgestellten geheimen Datenworte aus dem Inhalt der übertragenen Datenworte des Datenfeldes berechnet wird.

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

- DE 102012210327 A1 [0010, 0011, 0012, 0013, 0014]
- DE 102010033229 A1 [0015, 0016]
- DE 102008046563 A1 [0017, 0019]
- US 2002/0174332 A1 [0020, 0021]

Patentansprüche

1. Verfahren zur Absicherung der Datenübertragung in einem Datenbus, über den Datenprotokolle von mindestens einem Sender an wenigstens einen Empfänger übermittelt werden, wobei die Datenprotokolle zur Übermittlung von physikalisch übertragbaren Nutzdaten und einer CRC-Prüfsumme ein Datenfeld mit vorgegebener Länge enthalten, **dadurch gekennzeichnet**, dass
- wenigstens ein geheimes Datenwort in dem Sender und dem Empfänger bereitgestellt wird, und
- die CRC-Prüfsumme aus den zu übertragenden Nutzdaten und dem geheimen Datenwort berechnet wird.

2. Verfahren nach Anspruch 1, bei welchem das geheime Datenwort mit einer Länge bereitgestellt wird, die größer ist als die Länge der CRC-Prüfsumme.

3. Verfahren nach Anspruch 1 oder 2, bei welchem das wenigstens eine geheime Datenwort mittels eines kryptographischen Verfahrens in Speichereinheiten des Senders und des Empfängers gespeichert wird.

4. Verfahren nach einem der vorhergehenden Ansprüche, bei welchem das geheime Datenwort nach einer vorgegebenen Anzahl von versendeten Datenprotokollen gegen ein anderes geheimes Datenwort ausgetauscht wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, bei welchem nach einer Übertragung eines kryptographischen abgesicherten Datenprotokolls vom Sender an den Empfänger das geheime Datenwort ausgetauscht wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, bei welchem nach einer Übertragung eines kryptographischen abgesicherten Datenprotokolls vom Empfänger an den Sender das geheime Datenwort ausgetauscht wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, bei welchem nach einer vorgegebenen Folge von fehlerhaft von dem Empfänger empfangenen Prüfsummen das geheime Datenwort ausgetauscht wird und dem Sender vom Empfänger der Austausch des geheimen Datenwortes mitgeteilt wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, bei welchem nach einer vorgegebenen Folge von fehlerhaft von dem Empfänger empfangenen Prüfsummen dieser Empfänger in einen Notbetrieb übergeht, in welchem keine Datenprotokolle von dem Empfänger akzeptiert werden.

9. Verfahren nach einem der vorhergehenden Ansprüche, bei welchem die Abfolge der zum Austausch bereitgestellten geheimen Datenworte vorab festgelegt und in dem Sender und dem Empfänger gespeichert wird.

10. Verfahren nach einem der vorhergehenden Ansprüche, bei welchem der Datenbus als CAN-Bus realisiert wird.

Es folgt eine Seite Zeichnungen

Anhängende Zeichnungen

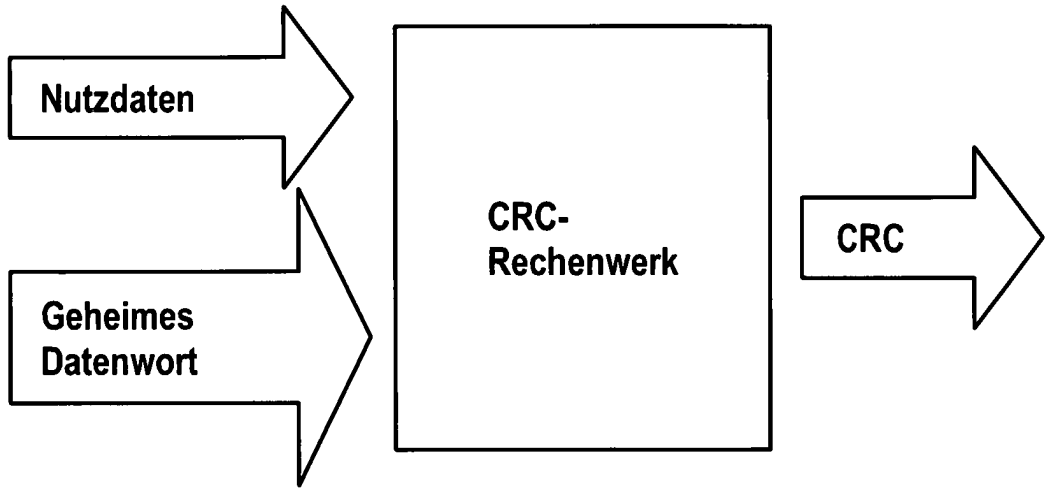


Fig. 1

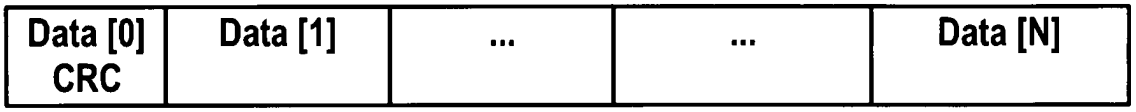


Fig. 2