



(10) **DE 10 2013 210 102 B4** 2024.08.01

(12)

## Patentschrift

(21) Aktenzeichen: **10 2013 210 102.3**  
(22) Anmeldetag: **29.05.2013**  
(43) Offenlegungstag: **26.06.2014**  
(45) Veröffentlichungstag  
der Patenterteilung: **01.08.2024**

(51) Int Cl.: **H04L 43/00 (2022.01)**  
**B60R 16/023 (2006.01)**  
**G06F 11/28 (2006.01)**  
**H04L 43/026 (2022.01)**  
**H04L 43/0888 (2022.01)**  
**H04L 43/16 (2022.01)**  
**H04L 47/24 (2022.01)**

Innerhalb von neun Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(30) Unionspriorität:  
**10-2012-0144900 12.12.2012 KR**

(73) Patentinhaber:  
**Hyundai Motor Company, Seoul, KR; Industry-Academic Cooperation Foundation, Gwangju, KR; SNU R&DB Foundation, Seoul, KR**

(74) Vertreter:  
**isarpatent - Patent- und Rechtsanwälte Barth Hassa Peckmann und Partner mbB, 80801 München, DE**

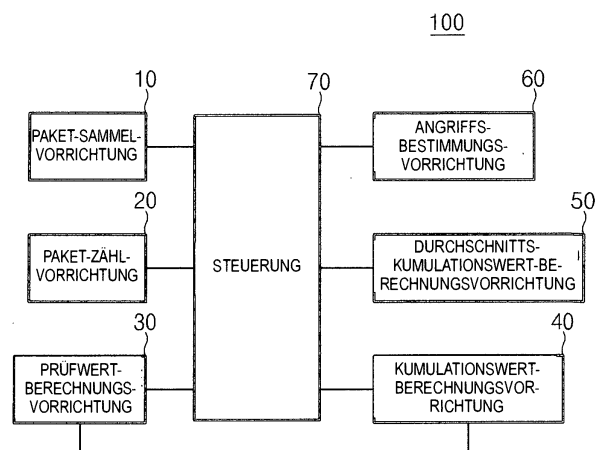
(72) Erfinder:  
**Ahn, Hyun Soo, Yongin, Kyonggi, KR; Lee, Chung Hi, Seoul, KR; Lee, Byoung Wook, Seoul, KR; Bae, Hyun Cheol, Suwon, Kyonggi, KR; No, Jong Seon, Seoul, KR; Kim, Ji Youp, Seoul, KR; Woo, Jun Young, Seoul, KR; Cho, Chang Min, Seoul, KR; Kim, Young Sik, Gwangju, KR; Moon, Young Sik, Seoul, KR**

(56) Ermittelter Stand der Technik:  
**siehe Folgeseiten**

(54) Bezeichnung: **VORRICHTUNG UND VERFAHREN ZUM ERFASSEN EINES ANGRIFFES AUF EIN FAHRZEUGSEITIGES NETZWERK**

(57) Hauptanspruch: Vorrichtung (100) zum Erfassen eines Angriffes auf ein fahrzeugseitiges Netzwerk unter einer fahrzeugseitigen Netzwerkumgebung, in der Vorrichtungen mit definierten Prioritäten für eine Paketübertragung mit einem fahrzeugseitigen Netzwerk-Bus verbunden sind, wobei die Vorrichtung (100) aufweist:  
eine Paket-Sammelvorrichtung (10), die eingerichtet ist, um über den fahrzeugseitigen Netzwerk-Bus übertragene Pakete zu sammeln;  
eine Paket-Zählvorrichtung (20), die eingerichtet ist, um die Anzahl von durch die Paket-Sammelvorrichtung (10) gesammelten Paketen kumulativ zu zählen;  
eine Prüfwert-Berechnungsvorrichtung (30), die eingerichtet ist, um einen Prüfwert auf der Grundlage einer Erzeugungszeitdifferenz von Paketen mit einer identischen ID zu berechnen;  
eine Kumulationswert-Berechnungsvorrichtung (40), die eingerichtet ist, um einen kumulierten Wert durch Summieren des durch die Prüfwert-Berechnungsvorrichtung (30) berechneten Prüfwerts und eines kurz zuvor berechneten Prüfwerts zu berechnen;  
eine Durchschnitts-Kumulationswert-Berechnungsvorrichtung (50), die eingerichtet ist, um einen durchschnittlichen kumulierten Wert durch Dividieren des durch die Kumulationswert-Berechnungsvorrichtung (40) berechneten

kumulierten Wertes durch einen durch die Paket-Zählvorrichtung (20) kumulativ gezählten Wert zu berechnen;  
eine Angriffs-Bestimmungsvorrichtung (60), die eingerichtet ist, um auf der Grundlage des durchschnittlichen kumulierten Wertes, der durch die Durchschnitts-Kumulationswert-Berechnungsvorrichtung (50) berechnet wird, zu bestimmen, ob ein Angriff erfolgt.



(56) Ermittelter Stand der Technik:

|           |                         |           |
|-----------|-------------------------|-----------|
| <b>DE</b> | <b>10 2008 018 001</b>  | <b>A1</b> |
| <b>US</b> | <b>2003 / 0 076 848</b> | <b>A1</b> |
| <b>WO</b> | <b>2012/ 091 436</b>    | <b>A2</b> |
| <b>JP</b> | <b>2007- 104 307</b>    | <b>A</b>  |

**Beschreibung**

## TECHNISCHES GEBIET

**[0001]** Der vorliegende Erfindungsgedanke betrifft eine Vorrichtung und ein Verfahren zum Erfassen eines Angriffes auf ein fahrzeugseitiges Netzwerk und insbesondere eine Vorrichtung und ein Verfahren zum vorzeitigen Erfassen von externen beliebigen Angriffen gegen ein fahrzeugseitiges Netzwerk.

## HINTERGRUND

**[0002]** Im Allgemeinen, da ein fahrzeugseitiges Netzwerk unabhängig von einem externen Netzwerk betrieben wird, gibt es keine Geräte zum Schützen von fahrzeugseitigen Netzwerkinformationen.

**[0003]** In letzter Zeit, da das fahrzeugseitige Netzwerk mit externen Netzwerken wie beispielsweise einem drahtlosen Kommunikationsnetzwerk (3G/4G), einem Bluetooth-Netzwerk und dergleichen verbunden werden kann und an ein Fahrzeug-Diagnose-Gerät angeschlossen werden kann, ist es wahrscheinlich, dass ein fahrzeugseitiges Netzwerk in negativer Weise beeinflusst wird. Das heißt, wenn ein böswilliger Angreifer von externen Netzwerken ein internes Netzwerk stört, tritt ein ernsthaftes Problem bei einem Betrieb des Fahrzeugs auf, was die Sicherheit der Passagiere gefährden kann.

**[0004]** Unterdessen werden die Eigenschaften (Paketgröße, Verzögerungszeit, Häufigkeit und dergleichen) von Internet-Paketen mit der gleichen IP-Adresse über die Zeit geändert und die Pakete weisen ebenfalls unregelmäßige und zufällige Eigenschaften auf. Daher bestimmt eine Technologie zum Erfassen eines Netzwerk-Angriffes im Allgemeinen auf der Grundlage der Anzahl von empfangenen Paketen pro Zeiteinheit, ob ein Angriff erfolgt.

**[0005]** Auf der anderen Seite weist die Gesamtheit der übertragenen Daten (Datenverkehr - Traffic), die in dem fahrzeugseitigen Netzwerk erzeugt wird, verschiedene Paketerzeugungsfrequenzen für jede ID auf, aber die Datenverkehre werden für jede ID relativ regelmäßig erzeugt. In diesem Fall, wenn zwei Pakete gleichzeitig erzeugt werden, wird eine Übertragungssequenz auf der Grundlage der Priorität bestimmt.

**[0006]** Daher kann, wenn Pakete mit einer ID bei einer hohen Geschwindigkeit erzeugt werden, ein Angriff von eindringenden Paketen mit einer höheren Priorität als die der ID in einem Netzwerk mit einer Frequenz ähnlich der Erzeugungsfrequenz von Paketen mit der ID nicht nur durch eine Analyse auf der Grundlage der Anzahl von empfangenen Paketen pro Zeiteinheit erfasst werden.

**[0007]** Das heißt, da IDs für einen Angriff mit einer höheren Priorität in ein Netzwerk anstelle einer normalen ID mit einer niedrigeren Priorität eingebracht werden, kann ein Angriff nicht nur durch ein Verfahren zum Zählen der Anzahl von Paketen erfasst werden.

**[0008]** Daher besteht eine Notwendigkeit für ein Datenverkehr-Analyseverfahren, das für Fahrzeug-Datenverkehre geeignet ist, das sich von einem Verfahren unterscheidet, das für eine Internet-Eindringungserfassung der verwendet wird.

**[0009]** Aus der JP 2007 - 104 307 A ist im Übrigen ein Verfahren zum Erkennen eines DOS-Angriffs bekannt, indem die Anzahl von übertragenen Datenpaketen pro Zeiteinheit überwacht wird und bei Überschreiten eines Schwellenwertes ein Angriff erkannt wird.

**[0010]** Die US 2003 / 0 076 848 A1 offenbart außerdem ein Verfahren zum Erkennen eines verteilten DOS-Angriffs (DDOS), wobei in einem Netzwerkgerät die übertragenen Datenpakete in unterschiedliche Klassen eingeteilt werden und wobei Abweichungen eines Datenstroms auf einen Angriff hinweisen.

## ZUSAMMENFASSUNG

**[0011]** Demzufolge ist der vorliegende Erfindungsgedanke gemacht worden, um die oben beschriebenen und im Stand der Technik auftretenden Probleme zu lösen, während die durch den Stand der Technik erreichten Vorteile beibehalten werden.

**[0012]** Es ist eine Aufgabe der vorliegenden Erfindung, eine Vorrichtung und ein Verfahren zum Erfassen eines Angriffes auf ein fahrzeugseitiges Netzwerk bereitzustellen, das Pakete für jede mit einem fahrzeugseitigen Netzwerk-Bus verbundenen Vorrichtung (IDs) kumulativ zählt, einen Prüfwert S jedes Mal kumuliert, wenn die Pakete kumulativ gezählt werden, um einen kumulierten Wert zu berechnen, und bestimmt, dass ein Angriff erfolgt, wenn ein durchschnittlicher kumulierter Wert, der durch Dividieren des kumulierten Wertes durch eine kumulative Zählung erhalten wird, einen ersten Schwellenwert nicht überschreitet.

**[0013]** Die Aufgabe wird gelöst durch eine Vorrichtung mit den Merkmalen des Anspruchs 1 und ein Verfahren mit den Merkmalen des Anspruchs 7. Vorteilhafte Weiterbildungen finden sich in den Unteransprüchen.

**[0014]** Eine weitere Ausgestaltung des vorliegenden Erfindungsgedankens umfasst eine Vorrichtung und ein Verfahren zum Erfassen eines Angriffes auf ein fahrzeugseitiges Netzwerk, das Pakete für jede Vor-

richtung (IDs), die in einem vorbestimmten Prioritätsbereich unter den mit einem fahrzeugseitigen Netzwerk-Bus verbundenen Vorrichtungen (IDs) umfasst ist, kumulativ zählt, einen Prüfwert  $S$  jedes Mal kumuliert, wenn die Pakete kumulativ gezählt werden, um einen kumulierten Wert zu berechnen, und bestimmt, dass ein Angriff erfolgt, wenn ein durchschnittlicher kumulierter Wert, der durch Dividieren des kumulierten Wertes durch eine kumulative Zählung erhalten wird, einen dritten Schwellenwert nicht überschreitet.

**[0015]** Eine Ausgestaltung des vorliegenden Erfindungsgedankens betrifft eine Vorrichtung zum Erfassen eines Angriffes auf ein fahrzeugseitiges Netzwerk unter der fahrzeugseitigen Netzwerkumgebung, in der Vorrichtungen mit definierten Prioritäten für eine Paketübertragung mit einem fahrzeugseitigen Netzwerk-Bus verbunden sind. Die Vorrichtung umfasst: eine Paket-Sammelvorrichtung, die eingerichtet ist, um über den fahrzeugseitigen Netzwerk-Bus übertragene Pakete zu sammeln; eine Paket-Zählvorrichtung, die eingerichtet ist, um die Anzahl von durch die Paket-Sammelvorrichtung gesammelten Pakete kumulativ zu zählen; eine Prüfwert-Berechnungsvorrichtung, die eingerichtet ist, um einen Prüfwert auf der Grundlage einer Erzeugungszeitdifferenz von Paketen mit einer identischen ID zu berechnen; eine Kumulationswert-Berechnungsvorrichtung, die eingerichtet ist, um einen kumulierten Wert durch Summieren des durch die Prüfwert-Berechnungsvorrichtung berechneten Prüfwertes und eines kurz zuvor berechneten Prüfwertes zu berechnen; eine Durchschnitts-Kumulationswert-Berechnungsvorrichtung, die eingerichtet ist, um einen durchschnittlichen kumulierten Wert durch Dividieren des durch die Kumulationswert-Berechnungsvorrichtung berechneten kumulierten Wertes durch einen durch die Paket-Zählvorrichtung kumulativ gezählten Wert zu berechnen; und eine Angriffs-Bestimmungsvorrichtung, die eingerichtet ist, um auf der Grundlage des durchschnittlichen kumulierten Wertes, der durch die Durchschnitts-Kumulationswert-Berechnungsvorrichtung berechnet wird, zu bestimmen, ob ein Angriff erfolgt.

**[0016]** Eine weitere Ausgestaltung des vorliegenden Erfindungsgedankens umfasst ein Verfahren zum Erfassen eines Angriffes auf ein fahrzeugseitiges Netzwerk unter der fahrzeugseitigen Netzwerkumgebung, in der Vorrichtungen mit definierten Prioritäten für eine Paketübertragung mit einem fahrzeugseitigen Netzwerk-Bus verbunden sind. Gemäß dem Verfahren werden über den fahrzeugseitigen Netzwerk-Bus übertragene Pakete durch eine Paket-Sammelvorrichtung gesammelt. Die Anzahl von gesammelten Paketen wird durch eine Paket-Zählvorrichtung kumulativ gezählt. Ein Prüfwert wird durch eine Prüfwert-Berechnungsvorrichtung auf der Grundlage einer Erzeugungszeitdifferenz von Paketen mit

einer identischen ID berechnet. Ein kumulierter Wert wird durch eine Kumulationswert-Berechnungsvorrichtung durch Summieren des berechneten Prüfwertes und eines kurz zuvor berechneten Prüfwertes berechnet. Ein durchschnittlicher kumulierter Wert wird durch einen durchschnittlichen kumulierten Wert durch Dividieren des berechneten kumulierten Wertes durch den kumulativ gezählten Wert berechnet. Es wird durch eine Angriffs-Bestimmungsvorrichtung auf der Grundlage des berechneten durchschnittlichen kumulierten Wertes bestimmt, ob ein Angriff erfolgt.

## KURZBESCHREIBUNG DER ZEICHNUNGEN

**[0017]** Die vorhergehenden und weiteren Merkmale des Erfindungsgedankens werden aus einer spezielleren Beschreibung von Ausführungsformen des Erfindungsgedankens ersichtlicher, wie dies in den beigefügten Zeichnungen dargestellt ist, in denen gleiche Bezugszeichen gleiche oder ähnliche Teile überall in den verschiedenen Ansichten bezeichnen können. Die Zeichnungen sind nicht notwendigerweise maßstabsgerecht, wobei stattdessen Wert auf die Veranschaulichung der Grundsätze der Ausführungsformen des Erfindungsgedankens gelegt wird.

**Fig. 1** zeigt ein Diagramm der Konfiguration einer Vorrichtung zum Erfassen eines Angriffes auf ein fahrzeugseitiges Netzwerk gemäß einem Ausführungsbeispiel des vorliegenden Erfindungsgedankens.

**Fig. 2A** zeigt ein Diagramm, das ein Beispiel eines fahrzeugseitigen Netzwerk-Busses darstellt, bei dem der vorliegende Erfindungsgedanke angewandt wird.

**Fig. 2B** zeigt ein Diagramm, das ein weiteres Beispiel eines fahrzeugseitigen Netzwerk-Busses darstellt, bei dem der vorliegende Erfindungsgedanke angewandt wird.

**Fig. 3** zeigt ein Diagramm, das ein Prinzip zum Erfassen eines Angriffes auf ein fahrzeugseitiges Netzwerk gemäß einem weiteren Ausführungsbeispiel des vorliegenden Erfindungsgedankens darstellt.

**Fig. 4** zeigt ein Flussdiagramm, das ein Verfahren zum Erfassen eines Angriffes auf ein fahrzeugseitiges Netzwerk gemäß noch einem weiteren Ausführungsbeispiel des vorliegenden Erfindungsgedankens darstellt.

## AUSFÜHRLICHE BESCHREIBUNG DER BEVORZUGTEN AUSFÜHRUNGSFORMEN

**[0018]** Die vorhergehenden und weiteren Merkmale des Erfindungsgedankens werden aus einer spezielleren Beschreibung von Ausführungsformen des Erfindungsgedankens ersichtlicher, wie dies in den

beigefügten Zeichnungen dargestellt ist, in denen gleiche Bezugszeichen gleiche oder ähnliche Teile überall in den verschiedenen Ansichten bezeichnen können. Die Zeichnungen sind nicht notwendigerweise maßstabsgerecht, wobei stattdessen Wert auf die Veranschaulichung der Grundsätze der Ausführungsformen des Erfindungsgedankens gelegt wird.

**[0019]** Nachstehend werden Ausführungsbeispiele des vorliegenden Erfindungsgedankens unter Bezugnahme auf die beigefügten Zeichnungen ausführlich beschrieben.

**[0020]** Fig. 1 zeigt ein Diagramm der Konfiguration einer Vorrichtung zum Erfassen eines Angriffes auf ein fahrzeugseitiges Netzwerk gemäß einem Ausführungsbeispiel des vorliegenden Erfindungsgedankens.

**[0021]** Wie in Fig. 1 dargestellt, kann eine Vorrichtung 100 zum Erfassen eines Angriffes auf ein fahrzeugseitiges Netzwerk gemäß einem Ausführungsbeispiel des vorliegenden Erfindungsgedankens eine Paket-Sammelvorrichtung 10, eine Paket-Zählvorrichtung 20, eine Prüfwert-Berechnungsvorrichtung 30, eine Kumulationswert-Berechnungsvorrichtung 40, eine Durchschnitts-Kumulationswert-Berechnungsvorrichtung 50, eine Angriffs-Bestimmungsvorrichtung 60 und eine Steuerung 70.

**[0022]** Die Vorrichtung zum Erfassen eines Angriffes auf ein fahrzeugseitiges Netzwerk (ADS: Angriffserfassungssystem), das die obigen Komponenten umfasst, kann in einem Gateway des fahrzeugseitigen Netzwerkes wie in Fig. 2A dargestellt, realisiert werden. Das ADS kann ebenfalls als eine separate Vorrichtung realisiert werden, die mit einem fahrzeugseitigen Netzwerk-Bus wie in Fig. 2B dargestellt verbunden ist.

**[0023]** Unter Beschreibung jeder Komponente kann die Paket-Sammelvorrichtung 10 zunächst über den fahrzeugseitigen Netzwerk-Bus übertragene Pakete sammeln. In diesem Fall können jeder mit dem fahrzeugseitigen Netzwerk verbundenen Vorrichtung (ECU: Elektronische Steuereinheiten - Electronic Control Units) eindeutige IDs zugewiesen werden und jede Vorrichtung kann Pakete, in die ihre eigene ID eingefügt ist, an das fahrzeugseitige Netzwerk übertragen.

**[0024]** Weiter kann die Paket-Zählvorrichtung 20 die Anzahl von durch die Paket-Sammelvorrichtung 10 gesammelten Paketen kumulativ zählen. Das heißt, die Paket-Zählvorrichtung 20 kann die durch die Paket-Sammelvorrichtung 10 gesammelten Pakete in jede ID klassifizieren und dann die Anzahl von Paketen für jede ID kumulativ zählen.

**[0025]** Darüber hinaus kann die Paket-Zählvorrichtung 20 die durch die Paket-Sammelvorrichtung 10 gesammelten Pakete in jede ID unter der Steuerung der Steuerung 70 klassifizieren und dann die Pakete der IDs mit einer vorbestimmten Priorität für jede ID kumulativ zählen.

**[0026]** Als nächstes kann die Prüfwert-Berechnungsvorrichtung 30 einen Prüfwert S auf der Grundlage einer Differenz zwischen einer aktuellen Zeit  $t_c$  und einer Zeit  $T_{ID}$ , bei der das Paket der entsprechenden ID kurz zuvor erzeugt worden ist, erzeugen. Das heißt, die Prüfwert-Berechnungsvorrichtung 30 berechnet den Prüfwert S unter Verwendung der folgenden Gleichung 1.

$$S = \log_2(t_c - t_{ID}) \quad [\text{Gleichung 1}]$$

**[0027]** Die Prüfwert-Berechnungsvorrichtung 30 kann die Zeiten, bei denen Pakete für jede ID erzeugt werden, aktualisieren.

**[0028]** Als nächstes kann die Kumulationswert-Berechnungsvorrichtung 40 einen kumulierten Wert  $A = A + S$  durch Summieren eines durch die Prüfwert-Berechnungsvorrichtung 30 berechneten Prüfwerts und eines kurz zuvor berechneten Prüfwerts berechnen. Hierbei bezeichnet A den kumulierten Wert.

**[0029]** Weiter kann die Durchschnitts-Kumulationswert-Berechnungsvorrichtung 50 einen durchschnittlichen kumulierten Wert durch Dividieren des durch die Prüfwert-Berechnungsvorrichtung 30 berechneten kumulierten Wertes durch einen durch die Paket-Zählvorrichtung 20 berechneten Wert (die Anzahl von kumulativen Paketen der entsprechenden ID) berechnen.

**[0030]** Anschließend kann die Angriffs-Bestimmungsvorrichtung 60 bestimmen, dass ein Angriff erfolgt, wenn der durch die Durchschnitts-Kumulationswert-Berechnungsvorrichtung 50 berechnete durchschnittliche kumulierte Wert einen Schwellenwert nicht überschreitet.

**[0031]** Indessen kann die Steuerung 70 jede Komponente steuern. Insbesondere kann die Steuerung 70 jede Komponente gemäß einer Richtlinie zum Erfassen eines Angriffes auf ein fahrzeugseitiges Netzwerk einzeln steuern.

**[0032]** Zum Beispiel, wenn es erfasst wird, ob ein Angriff gegen jede von allen mit dem fahrzeugseitigen Netzwerk-Bus verbundenen Vorrichtungen erfolgt, kann die Steuerung 70 eine entsprechende Steuerfunktion durchführen.

**[0033]** Als ein weiteres Beispiel, wenn es erfasst wird, ob ein Angriff gegen jede in einem vorbestimmten Prioritätsbereich umfasste Vorrichtung unter den

mit dem fahrzeugseitigen Netzwerk-Bus verbundenen Vorrichtungen erfolgt, kann die Steuerung 70 eine entsprechende Steuerfunktion durchführen.

**[0034]** Gemäß einem Ausführungsbeispiel des vorliegenden Erfindungsgedankens wird der kumulierte Wert durch Berechnen eines Logarithmus einer Differenz zwischen einer Zeit, wenn ein Paket mit einer bestimmten ID kurz zuvor erzeugt worden ist, und einer Zeit, wenn das Paket aktuell wieder erzeugt wird, kumuliert.

**[0035]** Mit anderen Worten steht die Zeitdifferenz zwischen der Erzeugung der Pakete der gleichen IDs in engem Zusammenhang mit einem Wahrscheinlichkeitswert, dass ein Paket der entsprechenden ID erzeugt wird. Das heißt, eine ID mit einer hohen Erzeugungsfrequenz (eine ID mit einer hohen Erzeugungswahrscheinlichkeit) weist eine kurze Zeitdifferenz auf, während eine ID mit einer niedrigen Erzeugungsfrequenz (eine ID mit einer niedrigen Erzeugungswahrscheinlichkeit) eine große Zeitdifferenz aufweist.

**[0036]** Da die ID mit der hohen Erzeugungsfrequenz eine kurze Zeitdifferenz aufweist, können häufig kleine Werte hinzugefügt werden. Auf der anderen Seite, da die ID mit der niedrigen Erzeugungsfrequenz eine große Zeitdifferenz aufweist, können selten große Werte hinzugefügt werden.

**[0037]** Wenn diese Werte kumuliert werden und dann durch die Anzahl von Gesamthäufigkeiten der Paketerzeugung der entsprechenden ID dividiert werden, kann ein durchschnittlicher erwarteter Wert (nachstehend durchschnittlicher kumulierter Wert) erhalten werden und es kann auf der Grundlage des erhaltenen durchschnittlichen erwarteten Wertes bestimmt werden, ob externe Angriff durchgeführt werden.

**[0038]** Nachfolgend wird ein Prinzip unter Bezugnahme auf **Fig. 3** beschrieben, mit dem die Vorrichtung zum Erfassen eines Angriffes auf ein fahrzeugseitiges Netzwerk externe Angriffe gegen das fahrzeugseitige Netzwerk erfassen kann.

**[0039]** Wie in **Fig. 3** dargestellt, wird es als der normale Datenverkehr angenommen, dass ein Paket mit der ID = 2 alle 2 ms erzeugt wird. In diesem Fall wird es angenommen, dass ein externer Angreifer als einen Prioritätsangriff ein Paket mit der ID = 1, das eine höhere Priorität als die des Pakets mit der ID = 2 aufweist, entsprechend der Erzeugungsperiode des normalen Datenverkehrs injiziert, um die Übertragung des normalen Datenpakets mit der ID = 2 zu verhindern.

**[0040]** In diesem Fall, da die Gesamtzahl aller Pakete acht ist, kann nicht nachvollzogen werden,

ob ein Angriff durchgeführt wird, wenn lediglich das herkömmliche Verfahren zum Überprüfen der Anzahl von Paketen verwendet wird.

**[0041]** Jedoch kann ein Ausführungsbeispiel des vorliegenden Erfindungsgedankens die folgende Differenz in dem kumulativen Durchschnittswert erzeugen, um herauszufinden, ob die Angriffe gegen das fahrzeugseitige Netzwerk durchgeführt werden.

**[0042]** In dem Fall des normalen Datenverkehrs wird der durchschnittliche kumulierte Wert  $(\log_2 10^{-3} + 7 \times \log_2 2 \times 10^{-3})/8 = -9.09$ .

**[0043]** Auf der anderen Seite, in dem Fall des Prioritätsangriffes, wird der durchschnittliche kumulierte Wert  $(\log_2 10^{-3} + \log_2 3 \times 10^{-3} + 5 \times \log_2 2 \times 10^{-3} + \log_2 14 \times 10^{-3})/8 = -8.67$ .

**[0044]** **Fig. 4** zeigt ein Flussdiagramm eines Verfahrens zum Erfassen eines Angriffes auf ein fahrzeugseitiges Netzwerk gemäß einem Ausführungsbeispiel des vorliegenden Erfindungsgedankens darstellt.

**[0045]** Als erstes kann die Paket-Sammelvorrichtung 10 die über den fahrzeugseitigen Netzwerk-Bus übertragenen Pakete sammeln (401).

**[0046]** Als nächstes kann die Paket-Zählvorrichtung 20 die Anzahl von durch die Paket-Sammelvorrichtung 10 gesammelten Paketen kumulativ zählen. In diesem Fall kann die Paket-Zählvorrichtung 20 die durch die Paket-Sammelvorrichtung 10 gesammelten Pakete in jede ID klassifizieren und dann die Anzahl von Paketen für jede ID kumulativ zählen. Die Paket-Zählvorrichtung 20 kann die durch die Paket-Sammelvorrichtung 10 gesammelten Pakete in jede ID klassifizieren und dann die Pakete der IDs, die eine vorbestimmte Priorität für jede ID aufweisen, kumulativ zählen.

**[0047]** Weiter kann die Prüfwert-Berechnungsvorrichtung 30 einen Prüfwert auf der Grundlage einer Erzeugungszeitdifferenz der gleichen ID-Pakete berechnen (403).

**[0048]** Als nächstes kann die Kumulationswert-Berechnungsvorrichtung 40 einen kumulierten Wert durch Summieren des durch die Prüfwert-Berechnungsvorrichtung 30 berechneten Prüfwerts und eines kurz zuvor berechneten Prüfwerts berechnen (405).

**[0049]** Weiter kann die Angriffs-Bestimmungsvorrichtung 60 auf der Grundlage des durch die Durchschnitts-Kumulationswert-Berechnungsvorrichtung 50 berechneten durchschnittlichen kumulierten Wertes bestimmen, ob irgendwelche Angriffe erfolgen (406).

**[0050]** Das Verfahren kann jedes Mal durchgeführt werden, wenn ein Paket erzeugt wird, das heißt, jedes Mal, wenn ein Paket gezählt wird, um so zu bestimmen, ob der Angriff gegen das fahrzeugseitige Netzwerk durchgeführt wird.

**[0051]** Wie oben dargelegt wurde, können gemäß Ausführungsbeispielen des vorliegenden Erfindungsgedankens die Versuche, um den normalen Betrieb eines Fahrzeugs aufgrund einer absichtlich auftretenden Fehlfunktion eines Fahrzeugs zu verhindern, im Voraus blockiert werden, indem die externen Angriffe gegen den fahrzeugseitigen Netzwerk-Bus vorzeitig erfasst werden.

**[0052]** Ferner kann gemäß Ausführungsbeispielen des vorliegenden Erfindungsgedankens die fahrzeugseitige Kommunikationslast minimiert werden, indem externe Angriffe ohne Injizieren von zusätzlichen Daten in den fahrzeugseitigen Netzwerk-Bus erfasst werden.

**[0053]** Darüber hinaus kann gemäß Ausführungsbeispielen des vorliegenden Erfindungsgedankens eine zusätzliche Angriffswahrscheinlichkeit blockiert werden, indem vorzeitig ein Versuch zum Analysieren der fahrzeugseitigen Kommunikation erfasst wird (z.B. ein Analyseversuch auf der Grundlage der Injektion der zufälligen Pakete).

**[0054]** Obwohl der vorliegende Erfindungsgedanke unter Bezugnahme auf begrenzte Ausführungsbeispiele und Zeichnungen beschrieben wurde, ist der vorliegende Erfindungsgedanke nicht darauf beschränkt und kann auf verschiedene Weise innerhalb des Geistes des vorliegenden Erfindungsgedankens und der nachstehend beschriebenen Ansprüche durch einen Fachmann auf dem Gebiet geändert und abgewandelt werden.

#### BEZUGSZEICHEN VON JEDEM DER ELEMENTE IN DEN FIGUREN

|     |                                                                         |
|-----|-------------------------------------------------------------------------|
| 10  | Paket-Sammelvorrichtung                                                 |
| 20  | Paket-Zählvorrichtung                                                   |
| 30  | Prüfwert-Berechnungsvorrichtung                                         |
| 40  | Kumulationswert-Berechnungsvorrichtung                                  |
| 50  | Durchschnitts-Kumulationswert-Berechnungsvorrichtung                    |
| 60  | Angriffs-Bestimmungsvorrichtung                                         |
| 70  | Steuerung                                                               |
| 100 | ADS                                                                     |
| 401 | ÜBER DEN FAHRZEUGSEITIGEN<br>NETZWERK-BUS ÜBERTRAGENES<br>PAKET SAMMELN |

|      |                                                                                                                                                    |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 402  | DIE ANZAHL VON GESAMMELTEN<br>PAKETEN KUMULATIV ZÄHLEN                                                                                             |
| 403  | PRÜFWERT AUF DER GRUNDLAGE<br>DER ERZEUGUNGSZEITDIFFERENZ<br>DER GLEICHEN ID-PAKETE<br>BERECHNEN                                                   |
| 404  | KUMULIERTEN WERT DURCH SUM-<br>MIEREN DES BERECHNETEN<br>PRÜFWERTS UND DES KURZ<br>ZUVOR BERECHNETEN PRÜF-<br>WERTS BERECHNEN                      |
| 405  | DURCHSCHNITTlichen KUMU-<br>LIERTEN WERT DURCH DIVIDIEREN<br>DES BERECHNETEN KUMULIERTEN<br>WERTES DURCH DEN KUMULATIV<br>GEZÄHLTEN WERT BERECHNEN |
| 4 06 | BESTIMMEN, OB ANGRIFF<br>ERFOLGT; AUF DER GRUNDLAGE<br>DES BERECHNETEN DURCH-<br>SCHNITTlichen KUMULIERTEN<br>WERTES                               |

#### Patentansprüche

1. Vorrichtung (100) zum Erfassen eines Angriffes auf ein fahrzeugseitiges Netzwerk unter einer fahrzeugseitigen Netzwerkumgebung, in der Vorrichtungen mit definierten Prioritäten für eine Paketübertragung mit einem fahrzeugseitigen Netzwerk-Bus verbunden sind, wobei die Vorrichtung (100) aufweist:
  - eine Paket-Sammelvorrichtung (10), die eingerichtet ist, um über den fahrzeugseitigen Netzwerk-Bus übertragene Pakete zu sammeln;
  - eine Paket-Zählvorrichtung (20), die eingerichtet ist, um die Anzahl von durch die Paket-Sammelvorrichtung (10) gesammelten Paketen kumulativ zu zählen;
  - eine Prüfwert-Berechnungsvorrichtung (30), die eingerichtet ist, um einen Prüfwert auf der Grundlage einer Erzeugungszeitdifferenz von Paketen mit einer identischen ID zu berechnen;
  - eine Kumulationswert-Berechnungsvorrichtung (40), die eingerichtet ist, um einen kumulierten Wert durch Summieren des durch die Prüfwert-Berechnungsvorrichtung (30) berechneten Prüfwerts und eines kurz zuvor berechneten Prüfwerts zu berechnen;
  - eine Durchschnitts-Kumulationswert-Berechnungsvorrichtung (50), die eingerichtet ist, um einen durchschnittlichen kumulierten Wert durch Dividieren des durch die Kumulationswert-Berechnungsvorrichtung (40) berechneten kumulierten Wertes durch einen durch die Paket-Zählvorrichtung (20) kumulativ gezählten Wert zu berechnen;
  - eine Angriffs-Bestimmungsvorrichtung (60), die eingerichtet ist, um auf der Grundlage des durchschnittlichen kumulierten Wertes, der durch die Durch-

schnitts-Kumulationswert-Berechnungsvorrichtung (50) berechnet wird, zu bestimmen, ob ein Angriff erfolgt.

2. Vorrichtung nach Anspruch 1, wobei die Angriffs-Bestimmungsvorrichtung (60) eingerichtet ist, um zu bestimmen, dass der Angriff erfolgt, wenn der durchschnittliche kumulierte Wert einen Schwellenwert nicht überschreitet.

3. Vorrichtung nach Anspruch 1, wobei die Paket-Zählvorrichtung (20) eingerichtet ist, um die durch die Paket-Sammelvorrichtung (10) gesammelten Pakete in jede ID zu klassifizieren und dann die Anzahl von Paketen für jede ID kumulativ zu zählen.

4. Vorrichtung nach Anspruch 1, wobei die Paket-Zählvorrichtung (20) eingerichtet ist, um die durch die Paket-Sammelvorrichtung (10) gesammelten Pakete in jede ID zu klassifizieren und dann die Pakete der IDs mit einer vorbestimmten Priorität für jede ID kumulativ zu zählen.

5. Vorrichtung nach Anspruch 1, wobei die Prüf-wert-Berechnungsvorrichtung (30) eingerichtet ist, um den Prüfwert auf der Grundlage einer Differenz zwischen einer aktuellen Zeit  $t_c$  und einer Zeit  $t_{ID}$ , bei welcher ein Paket mit der identischen ID kurz zuvor erzeugt wird, zu erzeugen.

6. Vorrichtung nach Anspruch 5, wobei die Prüf-wert-Berechnungsvorrichtung (30) eingerichtet ist, um einen Prüfwert S unter Verwendung der folgenden [Gleichung A] zu berechnen.

$$S = \log_2(t_c - t_{ID}) \quad [\text{Gleichung A}]$$

7. Verfahren zum Erfassen eines Angriffes auf ein fahrzeugseitiges Netzwerk unter einer fahrzeug-seitigen Netzwerkkumgebung, in der Vorrichtungen mit definierten Prioritäten für eine Paketübertragung mit einem fahrzeugseitigen Netzwerk-Bus verbunden sind, wobei das Verfahren aufweist:  
Sammeln, durch eine Paket-Sammelvorrichtung (10), von Paketen, die über den fahrzeugseitigen Netzwerk-Bus übertragen werden;  
kumulatives Zählen, durch eine Paket-Zählvorrichtung (20), der Anzahl von gesammelten Paketen;  
Berechnen, durch eine Prüfwert-Berechnungsvorrichtung (30), eines Prüfwertes auf der Grundlage einer Erzeugungszeitdifferenz von Paketen mit einer identischen ID;  
Berechnen, durch eine Kumulationswert-Berechnungsvorrichtung (40), eines kumulierten Wertes durch Summieren des berechneten Prüfwertes und eines kurz zuvor berechneten Prüfwertes;  
Berechnen, durch eine Durchschnitts-Kumulationswert-Berechnungsvorrichtung (50), eines durchschnittlichen kumulierten Wertes durch Dividieren des berechneten kumulierten Wertes durch einen

kumulativ gezählten Wert; und  
Bestimmen, durch eine Angriffs-Bestimmungsvorrichtung (60), ob ein Angriff erfolgt, auf der Grundlage des berechneten durchschnittlichen kumulierten Wertes.

8. Verfahren nach Anspruch 7, wobei es in dem Bestimmen, ob der Angriff erfolgt, bestimmt wird, dass der Angriff erfolgt, wenn der durchschnittliche kumulierte Wert einen Schwellenwert nicht überschreitet.

9. Verfahren nach Anspruch 7, wobei in dem Zählen der Pakete die durch die Paket-Sammelvorrichtung (10) gesammelten Pakete in jede ID klassifiziert werden und dann die Anzahl von Paketen für jede ID kumulativ gezählt wird.

10. Verfahren nach Anspruch 7, wobei in dem Zählen der Pakete die durch die Paket-Sammelvorrichtung (10) gesammelten Pakete in jede ID klassifiziert werden und dann die Pakete mit IDs, die eine vorbestimmte Priorität aufweisen, für jede ID kumulativ gezählt werden.

11. Verfahren nach Anspruch 7, wobei in dem Berechnen des Prüfwertes der Prüfwert auf der Grundlage einer Differenz zwischen einer aktuellen Zeit  $t_c$  und einer Zeit  $t_{ID}$ , bei welcher ein Paket der identischen ID kurz zuvor erzeugt wird, erzeugt wird.

12. Verfahren nach Anspruch 11, wobei in dem Berechnen des Prüfwertes ein Prüfwert S unter Verwendung der folgenden [Gleichung B] berechnet wird.

$$S = \log_2(t_c - t_{ID}) \quad [\text{Gleichung B}]$$

Es folgen 4 Seiten Zeichnungen

Anhängende Zeichnungen

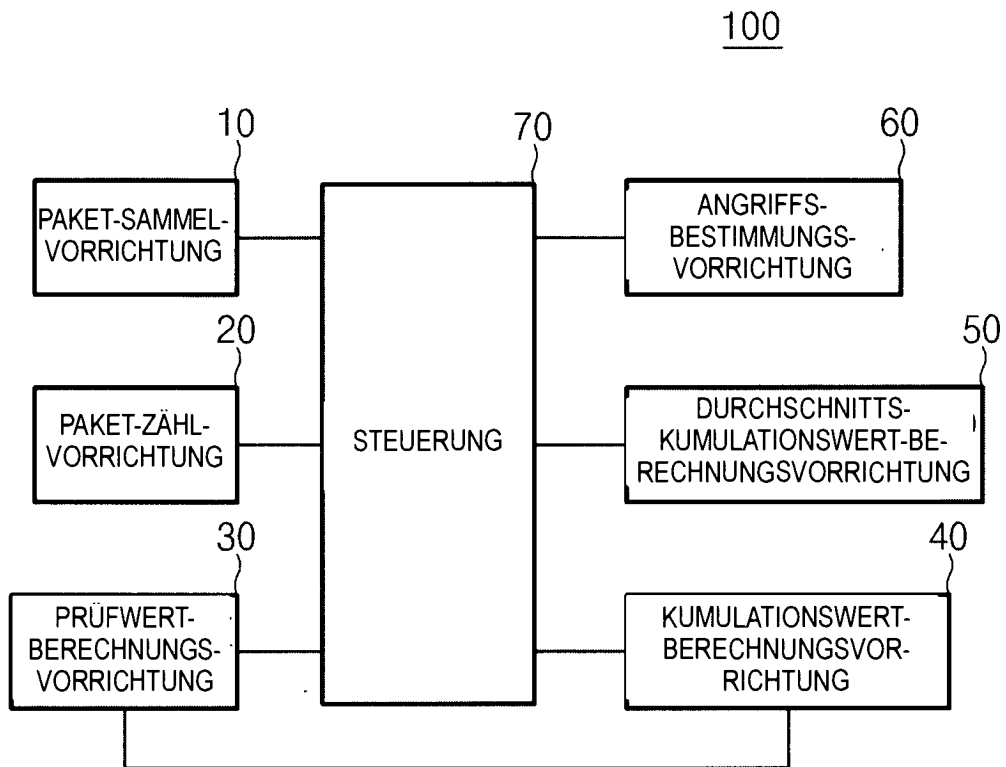


Fig.1

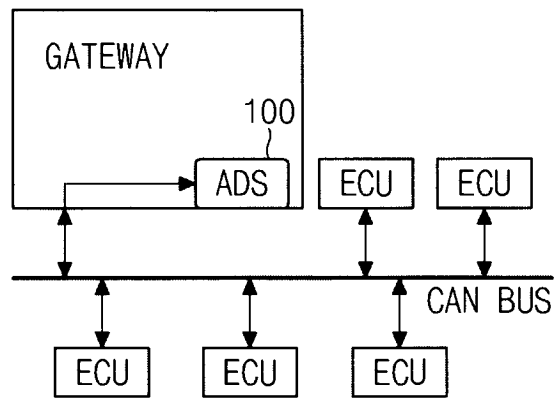


Fig. 2A

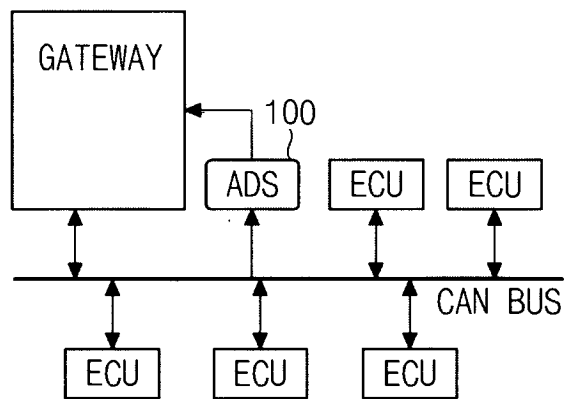


Fig. 2B

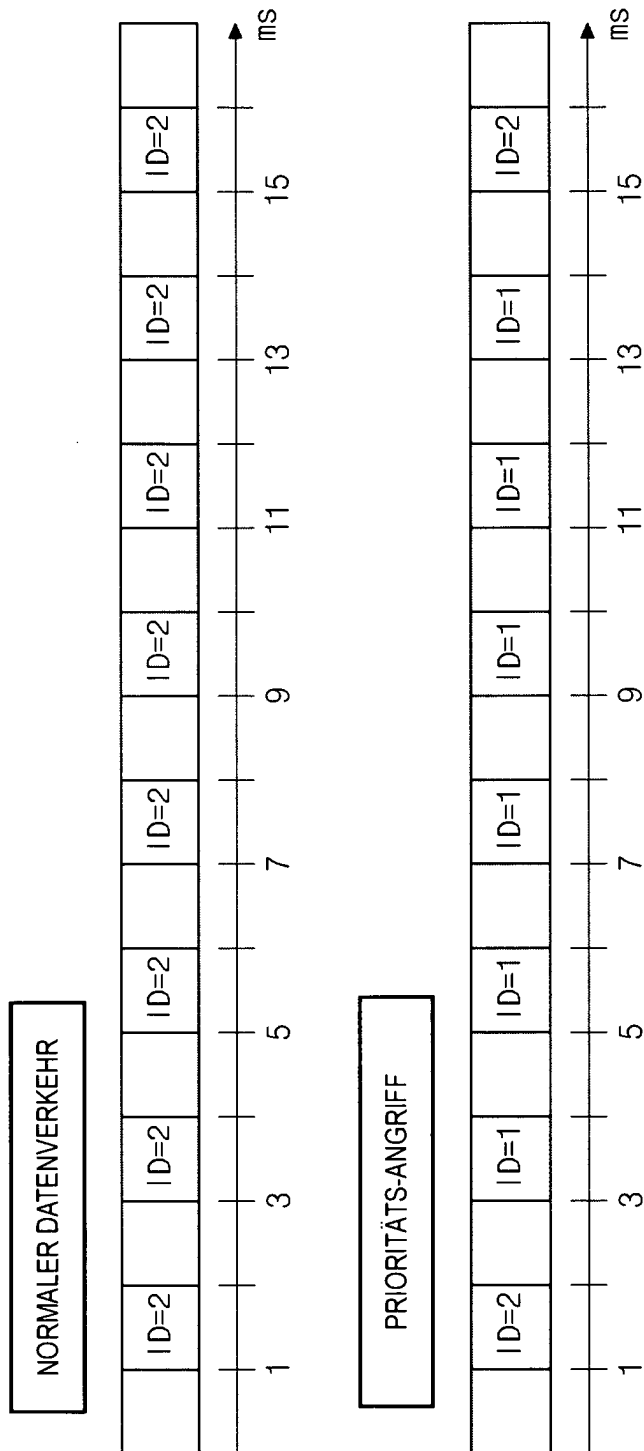


Fig.3

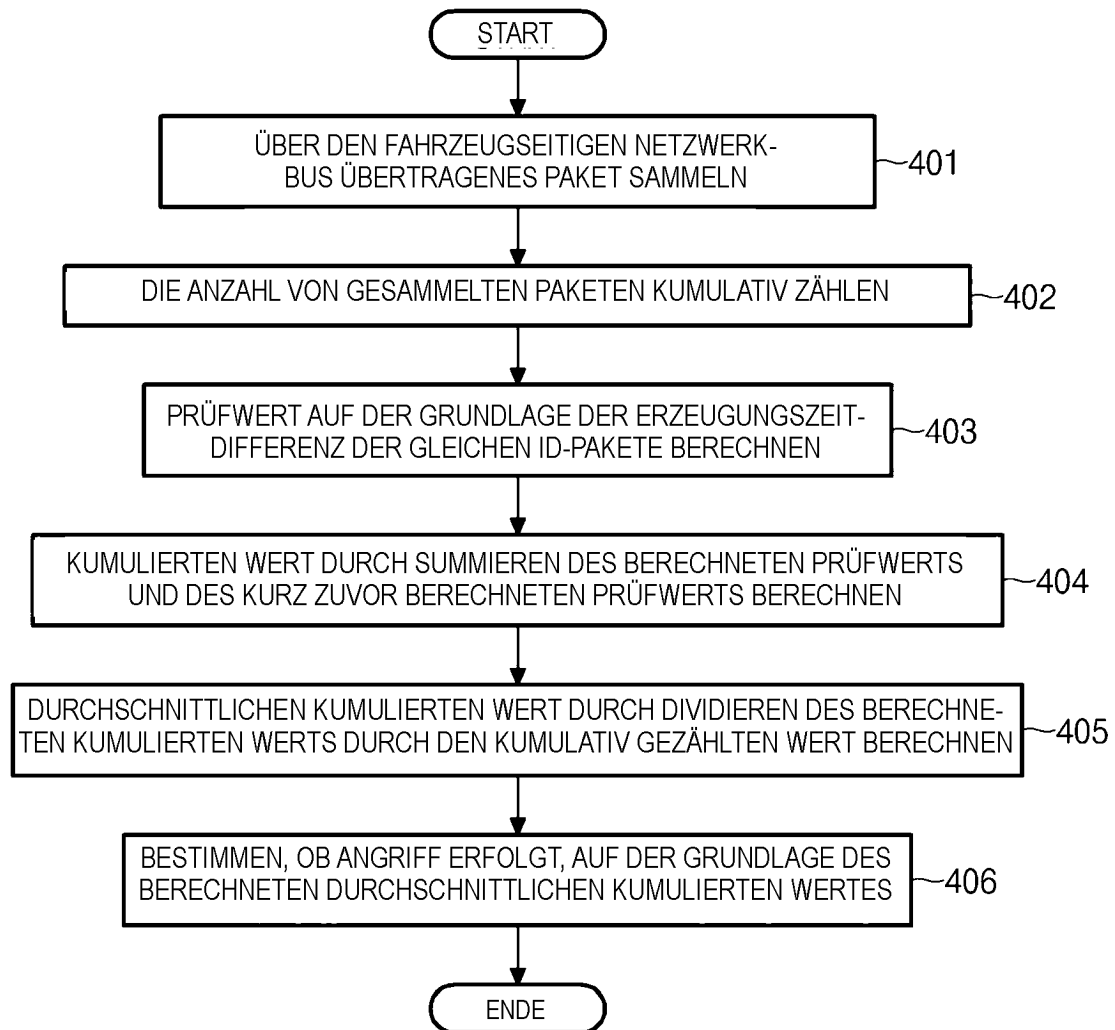


Fig. 4