(19) Deutsches Patent- und Markenamt

(10) **DE 10 2018 209 407 A1** 2019.12.19

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2018 209 407.1**
(22) Anmeldetag: **13.06.2018**
(43) Offenlegungstag: **19.12.2019**

(51) Int Cl.: ***H04L 12/26*** (2006.01)

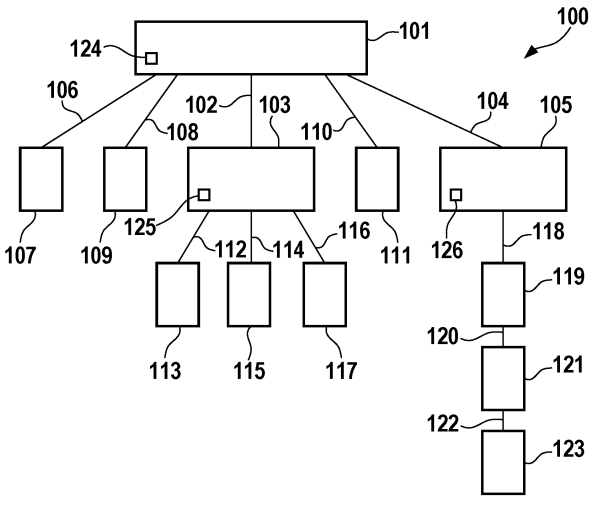
(71) Anmelder:
Robert Bosch GmbH, 70469 Stuttgart, DE

(72) Erfinder:
Wolfinger, Janin, 70439 Stuttgart, DE; Duplys, Paulius, 71706 Markgröningen, DE; Herrmann, Michael, 70469 Stuttgart, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Verfahren und Vorrichtung zur Behandlung einer Anomalie in einem Kommunikationsnetzwerk**

(57) Zusammenfassung: Vorrichtung und Verfahren zur Behandlung einer Anomalie in einem Kommunikationsnetzwerk (100), insbesondere eines Kraftfahrzeugs, dadurch gekennzeichnet, dass wenigstens ein Detektor (124, 125, 126) einen Datenstrom im Kommunikationsnetzwerk (100) analysiert, wobei der wenigstens eine Detektor (124, 125, 126) wenigstens eine Anomalie durch ein regelbasiertes Anomalieerkennungsverfahren erkennt, wenn wenigstens ein Parameter für ein Datenpaket des Datenstroms von einem Sollwert abweicht, wobei der wenigstens eine Detektor (124, 125, 126) Information über wenigstens eine erkannte Anomalie über das Kommunikationsnetzwerk (100) sendet.



Beschreibung

Technisches Gebiet

[0001] Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Behandlung einer Anomalie in einem Kommunikationsnetzwerk, ein Computerprogramm und ein maschinenlesbares Speichermedium.

Stand der Technik

[0002] Aus den nicht vorveröffentlichten DE 10 2017 210 787 und DE 10 2017 213 119 sind Verfahren zur Anomalieerkennung bekannt. Diese erfordern dedizierte Bauteile und eine statische Architektur, die zusätzlich zu einer zu überwachenden Kommunikationsnetzwerkstruktur hinzugefügt werden muss.

[0003] Wünschenswert ist es demgegenüber ein verbessertes Verfahren und eine verbesserte Vorrichtung anzugeben.

Offenbarung der Erfindung

[0004] Dies wird durch das Verfahren und die Vorrichtung nach den unabhängigen Ansprüchen erreicht.

[0005] Im Zusammenhang mit Aspekten der folgenden Ausführungen werden im Folgenden Abweichungen von einem Normalverhalten, die aus verschiedenen Gründen in einem realen Betrieb in Daten eines Systems zur Kommunikation der Daten auftreten können als Anomalie bezeichnet. Ursachen dafür können beispielsweise folgender Art sein:

Defekte oder ganz ausgefallene Sensoren liefern falsche oder gar keine Daten,

Bauteile des Systems sind beschädigt,

das System wurde durch eine externe Quelle (z. B. einen Hackerangriff) manipuliert.

[0006] Die Erkennung von Anomalien in Daten im Datenverkehr bei sowohl interner als auch externer Kommunikation wird mittels eines Network-Based Intrusion Detection Systems, NIDS, umgesetzt. Mit NIDS wird im Folgenden ein System bezeichnet, das den gesamten Datenverkehr im Kommunikationsnetz überwacht und analysiert, um alle Anomalien im internen und externen Datenaustausch zu erkennen. Ein NIDS, das um eine Komponente zur Prävention oder Reaktion auf erkannte Anomalien erweitert ist, wird im Folgenden als Network-Based Intrusion Detection and Prevention System, NIDPS, bezeichnet.

[0007] Herkömmliche NIDS oder NIDPS werden mit dedizierter Hardware realisiert. Entweder wird der Datenverkehr von einem zentralen Switch an eine separate NIDS oder NIDPS Komponente weitergeleitet, oder ausgewählte Switche werden um separate NIDS oder NIDPS Komponenten erweitert. In der ersten Lösung werden besonders schnelle Switchports verwendet um möglichst viel Datenverkehr an das NIDS oder NIDPS weiterzuleiten. Die zweite Lösung verwendet eine NIDS oder NIDPS Funktionalität direkt am Switch.

[0008] Das Verfahren zur Behandlung einer Anomalie in einem Kommunikationsnetzwerk, insbesondere eines Kraftfahrzeugs, sieht demgegenüber vor, dass wenigstens ein Detektor einen Datenstrom im Kommunikationsnetzwerk analysiert, wobei der wenigstens eine Detektor wenigstens eine Anomalie durch ein regelbasiertes Anomalieerkennungsverfahren erkennt, wenn wenigstens ein Parameter für ein Datenpaket des Datenstroms von einem Sollwert abweicht, und wobei der wenigstens eine Detektor Information über wenigstens eine erkannte Anomalie über das Kommunikationsnetzwerk sendet. Detektoren stellen Erkennungskomponenten für die regelbasierte Anomalieerkennung dar. Diese Erkennungskomponente setzt eine Kernaufgabe eines Angrifferkennungssystem, insbesondere eines NDIS, um. Die Kommunikation des Detektors über das Kommunikationsnetzwerk ermöglicht eine Separierung der Erkennungskomponente und deren Anordnung auf unterschiedlichen Geräten in dem überwachten Kommunikationsnetzwerk selbst. Dadurch wird ein separiertes NIDS beispielsweise in einem Automotive Ethernet Netzwerk realisiert. Durch die Separierung entsteht eine bezüglich Speicherbedarf oder Bedarf an Rechenressourcen kleine Einheit, die auf einem Steuergerät im Automotive Ethernet Netzwerk zusätzlich zu dessen anderen Aufgaben angeordnet werden kann. Die Kommunikation erfolgt über das bestehende Kommunikationsnetzwerk. Dedizierte Hardware für den Detektor oder eine zusätzliche Kommunikationsinfrastruktur sind nicht erforderlich.

[0009] Vorteilhafterweise ist vorgesehen, dass wenigstens ein Aktor Information über wenigstens eine vom wenigstens einen Detektor erkannte Anomalie über das Kommunikationsnetzwerk empfängt, und wobei der wenigstens eine Aktor abhängig von der Information über die wenigstens eine vom wenigstens einen Detektor erkannte Anomalie wenigstens eine Gegenmaßnahme zur Behandlung der Anomalie auslöst. Aktoren stellen eine Reaktionskomponente für die regelbasierte Anomalieerkennung und -behandlung dar. Diese Komponente setzt eine weitere Kernaufgabe des Angrifferkennungssystems um. Die Kommunikation zwischen Detektor und Aktor über das Kommunikationsnetzwerk ermöglicht eine Separierung dieser Komponenten auf unterschiedliche Geräte in dem überwachten Kommunikationsnetzwerk selbst. Dadurch wird ein separiertes NIDPS beispielsweise in dem Automotive Ethernet Netzwerk

realisiert, in dem es möglich ist, auf erkannte Anomalien sofort zu reagieren. Dedizierte Hardware oder eine zusätzliche Kommunikationsinfrastruktur sind dafür nicht erforderlich.

[0010] Vorteilhafterweise ist vorgesehen, dass wenigstens ein Aggregator Information über wenigstens eine erkannte Anomalie von wenigstens einem Detektor empfängt und wenigstens eine erkannte Anomalie über das Kommunikationsnetzwerk an wenigstens einen Aktor sendet. Der Aggregator stellt eine weitere Komponente, die Aggregationskomponente, dar, die Information über erkannte Anomalien von Detektoren aus verschiedenen Teilnetzwerken des Kommunikationsnetzwerks oder von verschiedenen Detektoren des Kommunikationsnetzwerks sammelt und an Aktoren weiterleitet. Dies ermöglicht es, Information über Anomalien in unterschiedlichen Teilnetzwerken auszutauschen. Dazu wird der Aggregator beispielsweise an einer Verbindungsstelle der Teilnetzwerke im Kommunikationsnetzwerk angeordnet.

[0011] Vorteilhafterweise ist vorgesehen, dass wenigstens zwei Detektoren Datenpakete des Datenstroms auf verschiedenen Geräten im Kommunikationsnetzwerk und/oder in demselben Teilnetzwerk analysieren. Dadurch wird die Kernaufgabe der Erkennung, d.h. die Erkennungskomponente, in diesem Teilnetzwerk verteilt auf mehrere Geräte ausgeführt. Dies reduziert den Bedarf an Rechenleistung, Arbeitsspeicher und oder Speicher, auf den einzelnen Geräten, auf denen der jeweilige Detektor ausgeführt wird.

[0012] Vorteilhafterweise ist vorgesehen, dass wenigstens zwei, auf unterschiedlichen Geräten im Kommunikationsnetzwerk und/oder auf unterschiedlichen Geräten in zwei verschiedenen Teilnetzwerken des Kommunikationsnetzwerks angeordnete Aktoren wenigstens eine Gegenmaßnahme auslösen. Dadurch wird die Kernaufgabe der Reaktion, d.h. die Reaktionskomponente, im Kommunikationsnetzwerk verteilt ausgeführt. Die Reaktion findet dadurch unmittelbar auf dem Gerät statt. Zusätzliche dedizierte Hardware ist nicht nötig.

[0013] Vorteilhafterweise ist vorgesehen, dass wenigstens zwei, auf unterschiedlichen Geräten im Kommunikationsnetzwerk und/oder auf unterschiedlichen Geräten in zwei verschiedenen Teilnetzwerken des Kommunikationsnetzwerks angeordnete Aggregatoren Information über erkannte Anomalien aggregieren, wobei ein weiterer Aggregator diese Information über erkannte Anomalien von den wenigstens zwei Aggregatoren aggregiert. Dies stellt eine hierarchische Aggregation in einem hierarchischen Kommunikationsnetzwerk dar. Dadurch sind komplexe hierarchische Strukturen des Kommunikationsnetzwerks besonders effizient überwachbar.

[0014] Vorteilhafterweise ist vorgesehen, dass eine Schnittstelle erkannte Anomalien insbesondere an ein Backend kommuniziert und/oder Anweisungen insbesondere von einem Backend empfängt. Eine weitere Kernaufgabe, die Kommunikation mit dem Backend, d.h. das Bereitstellen von Information über erkannte Anomalien wird dadurch realisiert. Anweisungen, die beispielsweise von einem Anwender oder automatisiert aus den erkannten Anomalien abgeleitet werden, können so zurückgeführt werden. Dies ermöglicht es, bezüglich der Rechenzeit, des Speicherplatzes oder des Arbeitsspeichers aufwändige Berechnungen außerhalb des zu überwachenden Kommunikationsnetzes vorzunehmen, oder von außerhalb des zu überwachenden Kommunikationsnetzes Einfluss zu nehmen.

[0015] Vorteilhafterweise ist vorgesehen, dass der Datenstrom zwischen Steuergeräten innerhalb wenigstens eines Teilnetzwerks des Kommunikationsnetzwerks in einem Detektor analysiert wird, der auf einem dieser Steuergeräte angeordnet ist und/oder dass der Datenstrom zwischen Steuergeräten aus verschiedenen Teilnetzwerken des Kommunikationsnetzwerks, die über ein Gateway oder Steuergerät miteinander verbunden sind, um einen Detektor analysiert wird, der auf dem Gateway oder diesem Steuergerät angeordnet ist. Dadurch ist eine hierarchische Überwachung möglich. Diese Anordnung ist in Kraftfahrzeugen mit stark hierarchischen Kommunikationsnetzwerken besonders vorteilhaft.

[0016] Vorteilhafterweise ist vorgesehen, dass wenigstens ein Detektor und/oder wenigstens ein Aggregator innerhalb wenigstens eines Teilnetzwerks des Kommunikationsnetzwerks verteilt auf mehreren Steuergeräten ausgeführt wird und/oder verteilt auf wenigstens einem Steuergerät und wenigstens einem Gateway ausgeführt wird. Diese verteilte Ausführung ermöglicht den Einsatz auf Steuergeräten oder Gateways mit geringer Anforderung an Rechenressourcen, beispielsweise auf embedded Hardware.

[0017] Vorteilhafterweise ist vorgesehen, dass einer der Aktoren mehreren weiteren Aktoren Anweisungen zu wenigstens einer Gegenmaßnahme über das Kommunikationsnetzwerk sendet. Durch diese hierarchische Anordnung der Aktoren wird die Gegenmaßnahme koordiniert ausgeführt.

[0018] Zudem ist ein Computerprogramm vorgesehen, das eingerichtet ist, ein derartiges Verfahren auszuführen, wenn es auf einem Computer ausgeführt wird. Ein maschinenlesbares Speichermedium, auf dem das Computerprogram gespeichert ist, ist ebenfalls vorgesehen.

[0019] Bezüglich der Vorrichtung zur Behandlung der Anomalie im Kommunikationsnetzwerk ist vorgesehen, dass wenigstens ein Detektor eingerichtet

ist, einen Datenstrom im Kommunikationsnetzwerk zu analysieren, wobei der wenigstens eine Detektor eingerichtet ist, wenigstens eine Anomalie durch ein regelbasiertes Anomalieerkennungsverfahren zu erkennen, wenn wenigstens ein Parameter für ein Datenpaket des Datenstroms von einem Sollwert abweicht, wobei der wenigstens eine Detektor eingerichtet ist, Information über wenigstens eine erkannte Anomalie über das Kommunikationsnetzwerk zu senden. Damit lässt sich die Detektion der Anomalien in einem Kommunikationsnetzwerk in ohnehin vorhandener embedded Hardware integrieren.

[0020] Vorteilhafterweise ist wenigstens ein Aktor eingerichtet, Information über wenigstens eine vom Detektor erkannte Anomalie über das Kommunikationsnetzwerk zu empfangen, und wobei der wenigstens eine Aktor eingerichtet ist, abhängig von der Information über die wenigstens eine vom Detektor erkannte Anomalie wenigstens eine Gegenmaßnahme zur Behandlung der Anomalie auszulösen. Damit lässt sich die Reaktion auf Anomalien in einem Kommunikationsnetzwerk in ohnehin vorhandener embedded Hardware integrieren.

[0021] Vorteilhafterweise ist wenigstens ein Aggregator eingerichtet, Information über wenigstens eine erkannte Anomalie von wenigstens einem Detektor zu empfangen und wenigstens eine erkannte Anomalie über das Kommunikationsnetzwerk an wenigstens einen Aktor zu senden. Dies stellt eine insbesondere für hierarchische Kommunikationsnetzwerke besonders geeignete Ausführung der Vorrichtung dar.

[0022] Weitere vorteilhafte Ausgestaltungen ergeben sich aus der folgenden Beschreibung und der Zeichnung. In der Zeichnung zeigt

Fig. 1 schematisch Teile eines Kommunikationsnetzwerks gemäß einer ersten Ausführungsform,

Fig. 2 schematisch Teile eines Kommunikationsnetzwerks gemäß einer zweiten Ausführungsform,

Fig. 3 schematisch Teile eines Kommunikationsnetzwerks gemäß einer dritten Ausführungsform,

Fig. 4 schematisch Teile eines Kommunikationsnetzwerks gemäß einer vierten Ausführungsform,

Fig. 5 schematisch Teile eines Kommunikationsnetzwerks gemäß einer fünften Ausführungsform,

Fig. 6 schematisch Teile eines Datenflusses in einem Kommunikationsnetzwerk.

[0023] Im Folgenden werden Aspekte einer Vorrichtung zur Behandlung einer Anomalie in einem Kommunikationsnetzwerk anhand eines Kommunikationsnetzwerks beschrieben das nach einer Version des Ethernet-Standards IEEE 802.3 aufgebaut ist. Eine Anwendung in anderen Kommunikationsnetzwerken ist ebenfalls möglich.

[0024] **Fig. 1** zeigt schematisch Teile eines derartigen Kommunikationsnetzwerks **100** gemäß einer ersten Ausführungsform für ein Kraftfahrzeug.

[0025] Das Kommunikationsnetzwerks **100** ist hierarchisch aufgebaut und umfasst ein zentrales Gateway **101** das über eine erste Ethernet-Verbindung **102** direkt mit einem ersten Domain-Steuergerät **103** und über eine zweite Ethernet-Verbindung **104** direkt mit einem zweiten Domain-Steuergerät **105** verbunden ist. Das Gateway **101** ist über eine dritte Ethernet-Verbindung **106** direkt mit einem ersten Steuergerät **107** verbunden. Das Gateway **101** ist über eine vierte Ethernet-Verbindung **108** direkt mit einem zweiten Steuergerät **109** verbunden. Das Gateway **101** ist über eine fünfte Ethernet-Verbindung **110** direkt mit einem dritten Steuergerät **111** verbunden. Das Gateway und diese Steuergeräte bilden ein erstes Teilnetzwerk des Kommunikationsnetzwerks **100**, dessen Teile nur über das Gateway **101** untereinander kommunizieren können.

[0026] Das erste Domain-Steuergerät **103** ist über eine sechste Ethernet-Verbindung **112** direkt mit einem vierten Steuergerät **113** verbunden. Das erste Domain-Steuergerät **103** ist über eine siebte Ethernet-Verbindung **114** direkt mit einem fünften Steuergerät **115** verbunden. Das erste Domain-Steuergerät **103** ist über eine achte Ethernet-Verbindung **116** direkt mit einem sechsten Steuergerät **117** verbunden. Diese Steuergeräte bilden ein zweites Teilnetzwerk, dessen Teile nur über das erste Domain-Steuergerät **103** untereinander kommunizieren können.

[0027] Das zweite Domain-Steuergerät **105** ist über eine neunte Ethernet-Verbindung **118** direkt mit einem siebten Steuergerät **119** verbunden. Das siebte Steuergerät **119** ist über eine zehnte Ethernet-Verbindung **120** direkt mit einem achten Steuergerät **121** verbunden. Das achte Steuergerät **122** ist über eine elfte Ethernet-Verbindung **122** direkt mit einem neunten Steuergerät **123** verbunden. Das neunte Steuergerät **123** ist über das achte Steuergerät **121** und das siebte Steuergerät **119** mit dem zweiten Domain-Steuergerät **105** verbunden. Diese Steuergeräte bilden ein drittes Teilnetzwerk.

[0028] In Zusammenhang mit den Verbindungen sind direkte Verbindungen solche, über die Daten ohne Zwischenschaltung weiterer Gateways, Switche oder Steuergeräte zwischen den direkt miteinander Verbundenen Enden der Verbindung übertragen werden.

[0029] Das Gateway und die Steuergeräte umfassen Prozessoren, Speicher, Arbeitsspeicher und Schnittstellen für eine Kommunikation über das Kommunikationsnetzwerk **100**. Im Speicher jedes der Steuergeräte sind Instruktionen gespeichert, bei deren Ausführung durch den Prozessor zusätzlich zur Kommunikation über Ethernet-Verbindungen von den Steuergeräten spezifische Aufgaben im Beispiel zum Betrieb des Kraftfahrzeugs ausgeführt werden. Das Gateway arbeitet Instruktionen zur Datenverbindung der Steuergeräte ab. Durch die Kommunikation entsteht ein Datenstrom, der Datenpakete umfasst. In einem Normalzustand werden Sollwerte beispielsweise bezüglich Zeitstempel, Auftretenshäufigkeit oder Frequenz bestimmter Datenpakete eingehalten. Die Datenpakete werden zur Erfüllung der spezifischen Aufgaben zwischen den Steuergeräten ausgetauscht.

[0030] Ein Domain-Steuergerät und die direkt mit dem Domain-Steuergerät verbundenen Steuergeräte bilden beispielsweise ein Teilnetzwerk aus spezifischen Steuergeräten mit gemeinsamer übergeordneter Aufgabe. Datenpakete werden dazu beispielsweise nur in diesem Teilenetzwerk gesendet.

[0031] Im Teilnetzwerk eines Domain-Steuergerätes kann Ethernet, insbesondere Automotive-Ethernet oder ein anderes automotive-typisches Bussystem verwendet werden, wie bspw. ein Controller Area Network, CAN, Bus.

[0032] Zur Behandlung von Anomalien im Kommunikationsnetz **100** ist unabhängig vom eingesetzten Standard eine Separierung von vier Kernaufgaben des NIDPS, nämlich Erkennung, Aggregation, Reaktion und Kommunikation auf verschiedene, optional alle Steuergeräte innerhalb des Kommunikationsnetzwerks **100** vorgesehen. Dies erfolgt mit dem Ziel ein NIDPS ausschließlich mittels bereits vorhandener Ressourcen zu realisieren.

[0033] Eine Erkennungskomponente, beispielsweise ein Detektor oder mehrere Detektoren analysiert den Datenstrom und erkennt Anomalien, wenn eine Abweichung vom Sollwert auftritt.

[0034] Eine Aggregationskomponente, beispielsweise ein Aggregator oder mehrere Aggregatoren, erhält Information über erkannte Anomalien z.B. einen Netzwerkstatus. Daraus kann eine Gesamtübersicht über das Teilnetzwerk generiert werden, die die erkannten Anomalien bewertet. Es ist weiterhin möglich, dass Aggregationskomponenten Nachrichten über Anomalien und Informationen an eine weitere Aggregationskomponente berichten und die Aggregation somit über mehrere Stufen erfolgt.

[0035] Eine Reaktionskomponente, beispielsweise ein Aktor oder mehrere Aktoren, kann aufgrund von erkannten Anomalien Gegenmaßnahmen auslösen. Die erkannten Anomalien werden der Reaktionskomponenten teils direkt von der Erkennungskomponente und teils von der Aggregationskomponente mitgeteilt. Gegenmaßnahmen können aktive Reaktionen, z. B. das Verändern oder Verwerfen von Ethernet Paketen, das Sperren von Ports oder das Ausschließen von Netzwerkteilnehmern oder passive Reaktionen z. B. die Benachrichtigung oder Warnung anderer Netzwerkteilnehmer sein.

[0036] Eine erste Ausführungsform betrifft die Separierung der Erkennungskomponente.

[0037] In der ersten Ausführungsform ist, wie in **Fig. 1** dargestellt, ein erster Detektor **124** vorgesehen. Der erste Detektor **124** ist ein Teil der Erkennungskomponente des NIDPS, der auf dem Gateway **101** ausgeführt wird. Der erste Detektor **124** analysiert den Datenstrom des ersten Teilnetzwerkes möglichst vollständig und erkennt mittels der regelbasierten Anomalieerkennung eine Anomalie, wenn wenigstens ein Parameter für ein Datenpaket des Datenstroms im ersten Teilnetzwerk von einem Sollwert abweicht. Der erste Detektor **124** sendet Information über eine erkannte Anomalie über das Kommunikationsnetzwerk **100**.

[0038] In der ersten Ausführungsform ist, wie in **Fig. 1** dargestellt, ein zweiter Detektor **125** vorgesehen. Der zweite Detektor **125** ist ein Teil der Erkennungskomponente des NIDPS, der auf dem ersten Domain Steuergerät **103** zusätzlich zu dessen spezifischer Aufgabe ausgeführt wird. Der zweite Detektor **125** analysiert den Datenstrom des zweiten Teilnetzwerkes möglichst vollständig und erkennt mittels einer regelbasierten Anomalieerkennung eine Anomalie, wenn wenigstens ein Parameter für ein Datenpaket des Datenstroms im zweiten Teilnetzwerk von einem Sollwert abweicht. Der zweite Detektor **125** sendet Information über eine erkannte Anomalie über das Kommunikationsnetzwerk **100**.

[0039] In der ersten Ausführungsform ist, wie in **Fig. 1** dargestellt, ein dritter Detektor **126** vorgesehen. Der dritte Detektor **126** ist ein Teil der Erkennungskomponente des NIDPS, der auf dem zweiten Domain Steuergerät **105** zusätzlich zu dessen spezifischen Aufgabe ausgeführt wird. Der dritte Detektor **126** analysiert den Datenstrom des dritten Teilnetzwerkes möglichst vollständig und erkennt mittels der regelbasierten Anomalieerkennung eine Anomalie, wenn wenigstens ein Parameter für ein Datenpaket des Datenstroms im dritten Teilnetzwerk von einem Sollwert abweicht. Der dritte Detektor **126** sendet Information über eine erkannte Anomalie über das Kommunikationsnetzwerk **100**.

[0040] Die anderen Komponenten des NIDPS sind beispielsweise zentral auf einem der anderen Steuergeräte angeordnet.

[0041] Durch diese verteilte Realisierung der Erkennungskomponente ist sichergestellt, dass der Netzwerkverkehr jedes Teilnetzwerkes möglichst vollständig analysiert werden kann. Dies wird gemäß der ersten Ausführungsform durch eine einzelne Erkennungskomponente innerhalb jedes Teilnetzwerkes realisiert.

[0042] Je nach Größe des Teilnetzwerkes und eines Netzwerktraffic ist die Analyse des gesamten Netzwerkverkehrs eines Teilnetzwerkes immer noch zu ressourcenintensiv. Deshalb kann die Erkennungskomponente gemäß einer zweiten Ausführungsform innerhalb eines Teilnetzwerkes weiter verteilt werden.

[0043] Dabei wird die Erkennungsfunktionalität individuell den Ressourcen der zur Verfügung stehenden Steuergeräte angepasst. Mehrere oder alle Steuergeräte eines Teilnetzwerks können demnach die Realisierung der Erkennungskomponente gemeinsam übernehmen.

[0044] Eine zweite Ausführungsform betrifft eine Verteilung der separierten Erkennungskomponente.

[0045] Im Falle des zweiten Teilnetzwerks wird diese, gemäß der in **Fig. 2** dargestellten zweiten Ausführungsform realisiert indem der zweite Detektor **125** als verteilter Detektor mit einem Teil **125a** auf dem ersten Domain-Steuergerät **103** und einem anderen Teil **125b** auf dem fünften Steuergerät **115** ausgeführt ist.

[0046] Im Falle des dritten Teilnetzwerks wird dies, gemäß der zweiten Ausführungsform realisiert indem der dritte Detektor **126** als verteilter Detektor mit einem ersten Teil **126a** auf dem zweiten Domain-Steuergerät **105**, einem zweiten Teil **126b** auf dem siebten Steuergerät **119**, einem dritten Teil **126c** auf dem achten Steuergerät **121** und einem vierten Teil **126d** auf dem neunten Steuergerät **123** ausgeführt ist.

[0047] Die Erkennung im ersten Teilnetzwerk wird durch einen einzigen Detektor **124** auf dem Gateway **101** realisiert. Die Erkennung im zweiten Teilnetzwerk wird auf zwei Steuergeräte aufgeteilt. Im dritten Teilnetzwerk sind alle Steuergeräte an der Erkennung beteiligt.

[0048] Die anderen Komponenten des NIDPS sind beispielsweise zentral auf einem der anderen Steuergeräte angeordnet.

[0049] Die übrigen Teile der zweiten Ausführungsform sind identisch zur ersten Ausführungsform ausgeführt. Für eine diesbezügliche Beschreibung der zweiten Ausführungsform wird auf die Beschreibung der ersten Ausführungsform verwiesen.

[0050] Eine dritte Ausführungsform betrifft eine Separierung der Aggregationskomponente.

[0051] Die Aggregationskomponente umfasst hierbei mehrere Aggregatoren, die individuell den Ressourcen der zur Verfügung stehenden Steuergeräte angepasst, im Kommunikationsnetzwerk **100** angeordnet werden. Mehrere oder alle Steuergeräte eines Teilnetzwerks können demnach die Realisierung der Aggregationskomponente gemeinsam übernehmen.

[0052] Für eine mehrstufige Aggregation werden Aggregatoren überall dort eingesetzt, wo es möglich und sinnvoll ist. Die Platzierung dieser Aggregatoren ist vollständig unabhängig von einer Netzwerktopologie des Kommunikationsnetzwerks **100**. Eine mögliche Verteilung der mehrstufigen Aggregatoren ist in **Fig. 3** dargestellten.

[0053] Ein erster Aggregator **127** ist auf dem ersten Steuergerät **107** angeordnet. Die Instruktionen für den ersten Aggregator **127** laufen zusätzlich zu den Aufgaben ab, die für den Betrieb des Kraftfahrzeugs auf dem ersten Steuergerät **107** ablaufen.

[0054] Ein zweiter Aggregator **128** ist auf dem vierten Steuergerät **113** angeordnet. Die Instruktionen für den zweiten Aggregator **128** laufen zusätzlich zu den Aufgaben ab, die für den Betrieb des Kraftfahrzeugs auf dem vierten Steuergerät **113** ablaufen.

[0055] Ein dritter Aggregator **129** ist auf dem fünften Steuergerät **115** angeordnet. Die Instruktionen für den dritten Aggregator **129** laufen zusätzlich zu den Aufgaben ab, die für den Betrieb des Kraftfahrzeugs auf dem fünften Steuergerät **115** ablaufen.

[0056] Ein vierter Aggregator **130** ist auf dem zweiten Domain-Steuergerät **105** angeordnet. Die Instruktionen für den vierten Aggregator **130** laufen zusätzlich zu den Aufgaben ab, die für den Betrieb des Kraftfahrzeugs auf dem zweiten Domain-Steuergerät **105** ablaufen.

[0057] Ein fünfter Aggregator **131** ist auf dem neunten Steuergerät **123** angeordnet. Die Instruktionen für den fünften Aggregator **131** laufen zusätzlich zu den Aufgaben ab, die für den Betrieb des Kraftfahrzeugs auf dem neunten Steuergerät **123** ablaufen.

[0058] Der erste Aggregator **127**, der zweite Aggregator **128**, der dritte Aggregator **129**, der vierte Aggregator **130** und der fünfte Aggregator **131** bilden eine erste Stufe der Aggregation. Die Aggregatoren der ersten Stufe senden aggregierte Information über erkannte Anomalien beispielsweise als Netzwerkzustand an Aggregatoren einer zweiten Stufe.

[0059] Die zweite Stufe wird im Beispiel von einem sechsten Aggregator **132**, der auf dem zweiten Steu-

ergerät **109** angeordnet ist, und von einem siebten Aggregator **133**, der auf dem achten Steuergerät **121** angeordnet ist, gebildet. Die Instruktionen für den sechsten Aggregator **132** laufen zusätzlich zu den Aufgaben ab, die für den Betrieb des Kraftfahrzeugs auf dem zweiten Steuergerät **109** ablaufen. Die Instruktionen für den siebten Aggregator **133** laufen zusätzlich zu den Aufgaben ab, die für den Betrieb des Kraftfahrzeugs auf dem achten Steuergerät **121** ablaufen.

[0060] Die Aggregatoren der zweiten Stufe aggregieren die Information von den Aggregatoren der ersten Stufe und senden diese aggregierte Information über erkannte Anomalien an wenigstens einen Aggregator einer dritten Stufe. Im Beispiel ist ein achter Aggregator **134** in der dritten Stufe vorgesehen, der auf dem dritten Steuergerät **111** angeordnet ist. Die Instruktionen für den achten Aggregator **134** laufen zusätzlich zu den Aufgaben ab, die für den Betrieb des Kraftfahrzeugs auf dem dritten Steuergerät **111** ablaufen.

[0061] Die anderen Komponenten des NIDPS sind beispielsweise zentral auf einem der anderen Steuergeräte angeordnet.

[0062] Das Kommunikationsnetzwerk **100** ist im Übrigen wie bei der ersten Ausführungsform aufgebaut. Für eine diesbezügliche Beschreibung der dritten Ausführungsform wird auf die Beschreibung der ersten Ausführungsform verwiesen.

[0063] Eine vierte Ausführungsform betrifft eine Separierung der Reaktionskomponente.

[0064] Die Reaktionskomponente umfasst hierbei, wie in **Fig. 4** dargestellt, mehrere Aktoren, die individuell den Ressourcen der zur Verfügung stehenden Steuergeräte angepasst, im Kommunikationsnetzwerk **100** angeordnet werden. Mehrere oder alle Steuergeräte eines Teilnetzwerks können demnach die Realisierung der Reaktionskomponente gemeinsam übernehmen.

[0065] Im Beispiel sind die Aktoren nach den Teilnetzwerken gruppiert.

[0066] Im ersten Teilnetzwerk ist ein erster Aktor **135** im Gateway **101** angeordnet. Die Instruktionen für den ersten Aktor **135** laufen zusätzlich zu den Aufgaben ab, die für den Betrieb des Kraftfahrzeugs auf dem Gateway **101** ablaufen.

[0067] Im ersten Teilnetzwerk ist ein zweiter Aktor **136** im ersten Steuergerät **107** angeordnet. Die Instruktionen für den zweiten Aktor **136** laufen zusätzlich zu den Aufgaben ab, die für den Betrieb des Kraftfahrzeugs auf dem ersten Steuergerät **107** ablaufen.

[0068] Im ersten Teilnetzwerk ist ein dritter Aktor **137** im dritten Steuergerät **111** angeordnet. Die Instruktionen für den dritten Aktor **137** laufen zusätzlich zu den Aufgaben ab, die für den Betrieb des Kraftfahrzeugs auf dem dritten Steuergerät **111** ablaufen.

[0069] Im zweiten Teilnetzwerk ist ein vierter Aktor **138** im ersten Domain-Steuergerät **103** angeordnet. Die Instruktionen für den vierten Aktor **138** laufen zusätzlich zu den Aufgaben ab, die für den Betrieb des Kraftfahrzeugs auf dem ersten Domain-Steuergerät **103** ablaufen.

[0070] Im dritten Teilnetzwerk ist ein fünfter Aktor **139** im zweiten Domain-Steuergerät **105** angeordnet. Die Instruktionen für den fünften Aktor **139** laufen zusätzlich zu den Aufgaben ab, die für den Betrieb des Kraftfahrzeugs auf dem zweiten Domain- Steuergerät **105** ablaufen.

[0071] Im dritten Teilnetzwerk ist ein sechster Aktor **140** im achten Steuergerät **121** angeordnet. Die Instruktionen für den sechsten Aktor **140** laufen zusätzlich zu den Aufgaben ab, die für den Betrieb des Kraftfahrzeugs auf dem achten Steuergerät **121** ablaufen.

[0072] Die anderen Komponenten des NIDPS sind beispielsweise auf einem der anderen Steuergeräte angeordnet. Das Kommunikationsnetzwerk **100** ist im Übrigen wie in der ersten Ausführungsform beschrieben aufgebaut.

[0073] Eine fünfte Ausführungsform betrifft eine Separierung und Verteilung aller Kernaufgaben des NIDPS. Aufgrund der Verteilung aller Kernaufgaben des NIDPS ist es besonders effizient möglich auf erkannte Anomalien unmittelbar zu reagieren. Durch das Nutzen der vorhandenen Hardware werden keine zusätzlichen Kosten erzeugt.

[0074] Wie in **Fig. 5** dargestellt, sind die zuvor beschriebenen Detektoren, Aggregatoren und Aktoren separat und verteilt angeordnet und ausgebildet.

[0075] Auf dem Gateway **101** sind der erste Detektor **124** und der erste Aktor **135** angeordnet. Auf dem ersten Steuergerät **107** sind der erste Aggregator **127** und der zweite Aktor **136** angeordnet. Auf dem zweiten Steuergerät **109** ist der sechste Aggregator **132** angeordnet. Auf dem dritten Steuergerät **111** sind der achte Aggregator **134** und der dritte Aktor **137** angeordnet. Auf dem vierten Steuergerät **113** ist der zweite Aggregator **128** angeordnet. Auf dem fünften Steuergerät **115** ist der dritte Aggregator **129** angeordnet. Auf dem ersten Domain-Steuergerät **103** ist der vierte Aktor **138** angeordnet. Auf dem zweiten Domain-Steuergerät **105** sind der dritte Detektor **126** und der fünfte Aktor **139** angeordnet.

[0076] Der verteilte Detektor im zweiten Teilnetz ist mit dem Teil **125a** auf dem ersten Domain-Steuergerät **103** und dem anderen Teil **125b** auf dem fünften Steuergerät **115** ausgeführt. Der verteilte Detektor im dritten Teilnetz ist mit dem ersten Teil **126a** auf dem zweiten Domain-Steuergerät **105**, dem zweiten Teil **126b** auf dem siebten Steuergerät **119**, dem dritten Teil **126c** auf dem achten Steuergerät **121** und dem vierten Teil **126d** auf dem neunten Steuergerät **123** ausgeführt.

[0077] Auf dem sechsten Steuergerät **117** ist eine Kommunikationskomponente **141** angeordnet. Die Kommunikationskomponente **141** übernimmt die Kommunikation des NIDPS zum Backend. Sie stellt dem Backend Informationen über erkannte Anomalien und den Netzwerkzustand zur Verfügung und erhält Anweisungen aus dem Backend.

[0078] Jede zuvor beschriebenen NIDPS Kernaufgabe vom NIDPS kann separiert und vollständig von einem der Steuergeräte realisiert werden. Es ist ebenfalls möglich, dass diese Kernaufgabe auf mehre Steuergeräte verteilt wird. Die Eignung eines Steuergerätes eine Kernaufgabe des NIDPS teilweise oder vollständig zu übernehmen kann an Hand von Eigenschaften wie zum Beispiel verfügbaren freie Ressourcen, Position in der Netzwerktopologie oder vorhandener Kommunikationsschnittstellen ermittelt werden.

[0079] In der fünften Ausführungsform ist eine derartige Separierung und Verteilung aller Kernaufgaben innerhalb eines Automotive-Netzwerkes exemplarisch dargestellt. Alle Steuergeräte und das Gateway sind an der Realisierung beteiligt und haben unterschiedliche Aufgabenteile zugewiesen bekommen. Diese beispielhaft dargestellte Verteilung lässt sich auf die verfügbaren Ressourcen jeder anderen Architektur anpassen und ist so individuell realisierbar.

[0080] Der Datenstrom zwischen Steuergeräten wird beispielsweise durch einen Detektor innerhalb wenigstens eines Teilnetzwerks des Kommunikationsnetzwerks analysiert. Der Datenstrom zwischen Steuergeräten aus verschiedenen Teilnetzwerken des Kommunikationsnetzwerks, die über ein Gateway oder Steuergerät miteinander verbunden sind, wird beispielsweise durch einen Detektor analysiert, der auf dem Gateway oder diesem Steuergerät angeordnet ist.

[0081] Allgemein werden die Kernaufgaben des NIDPS separiert. Zudem kann ein Detektor und/oder wenigstens ein Aggregator innerhalb wenigstens eines Teilnetzwerks des Kommunikationsnetzwerks verteilt auf mehreren Steuergeräten oder verteilt auf wenigstens einem Steuergerät und wenigstens einem Gateway ausgeführt werden.

[0082] Ein Datenfluss innerhalt des NIDPS ist in **Fig. 6** schematisch dargestellt.

[0083] Die Detektoren wirken als Erkennungskomponente zusammen. Die Aggregatoren wirken als Aggregationskomponente zusammen. Die Aktoren wirken als Reaktionskomponente zusammen. Die Kommunikationskomponente kommuniziert mit dem Backend.

[0084] In einem Schritt **601** wird der Datenstrom von der Erkennungskomponente analysiert und Information über eine Anomalie erkannt. Beispielsweise analysieren, wie in der zweiten und fünften Ausführungsform dargestellt zwei verteilte Detektoren **125a**, **125b** auf dem ersten Domain-Steuergerät **103** und dem fünften Steuergerät **115** den Datenstrom auf verschiedenen Geräten im Kommunikationsnetzwerk **100** in demselben Teilnetzwerk. Beispielsweise analysieren, wie in der ersten Ausführungsform dargestellt verschiedene Detektoren **124**, **125**, **126** den Datenstrom auf verschiedenen Geräten im Kommunikationsnetzwerk **100** in verschiedenen Teilnetzwerken.

[0085] Beispielsweise wird ein defekter oder ganz ausgefallener Sensor daran erkannt, dass falsche oder gar keine Daten vom Sensor gesendet werden. Es können auch defekte Bauteile oder Manipulation durch externe Quellen, die zu fehlerhaften Daten führen, erkannt werden. Zeitstempel, Auftretenshäufigkeit oder -abstand einzelner Datenpakete werden beispielsweise mit einem Sollwert verglichen, der einen Normalzustand charakterisiert. Allgemein wird eine regelbasierte Anomalieerkennung durchgeführt, die eine Abweichung von einem Sollwert erkennt.

[0086] In einem Schritt **602** wird Information über erkannte Anomalien von der Erkennungskomponente an die Aggregationskomponente gesendet.

[0087] In einem Schritt **603** wird Information über erkannte Anomalien von der Erkennungskomponente an die Reaktionskomponente gesendet.

[0088] In einem Schritt **604** aggregiert die Aggregationskomponente empfangene Information über Anomalien. Erkennen mehrere Detektoren eine Anomalie, wird deren Information vom Aggregator im Schritt **604** aggregiert. Die Information kann ausgewertet, bewertet oder nach Art und Weise der Anomalie sortiert und Aktoren zugeordnet werden.

[0089] In einem Schritt **605** wird aggregierte Information über erkannte Anomalien von der Aggregationskomponente an die Reaktionskomponente gesendet.

[0090] In einem Schritt **606** löst die Reaktionskomponente eine Gegenmaßnahme aus, die abhängt von der Information über erkannte Anomalien.

[0091] Ein erster Aspekt der Reaktion betrifft die direkte Reaktion auf eine erkannte Anomalie.

[0092] Ein Detektor der Erkennungskomponente sendet im Schritt **603** beispielsweise direkt Information über eine erkannte Anomalie mittels der zweiten Verbindung an einen Aktor der Reaktionskomponente.

[0093] Dadurch empfängt der Aktor vom Detektor direkt Information über eine erkannte Anomalie. Dieser Aktor löst im Beispiel abhängig von der Information über die erkannte Anomalie direkt eine Gegenmaßnahme zur Behandlung der Anomalie aus.

[0094] Ein zweiter Aspekt betrifft eine Aggregation von Information über Anomalien, und eine Reaktion aufgrund aggregierter Information. Dadurch empfängt der Aktor vom Aggregator Information über eine erkannte Anomalie. Dieser Aktor löst im Beispiel abhängig von der aggregierten Information über die erkannte Anomalie eine Gegenmaßnahme zur Behandlung der Anomalie aus. Damit führt beispielsweise eine von einem einzelnen Detektor nicht erkennbare Anomalie, die aber anhand aggregierter Information von mehreren Detektoren erkennbar ist, auch zu einer Reaktion.

[0095] Beispielsweis aggregieren, wie in der dritten und fünften Ausführungsform dargestellt, wenigstens zwei, auf unterschiedlichen Geräten im Kommunikationsnetzwerk **100** angeordnete Aggregatoren **127**, ..., **134** Information über erkannte Anomalien. Diese können hierarchisch ausgebildet sein, indem beispielsweise der Aggregator **134** einer höchsten Stufe, die Information über erkannte Anomalien von den Aggregatoren **127**, ..., **133** der niedrigeren Stufen aggregiert.

[0096] Beispielsweise lösen, wie in der vierten und fünften Ausführungsform dargestellt, wenigstens zwei, auf unterschiedlichen Geräten im Kommunikationsnetzwerk **100** angeordnete Aktoren **135**, ..., **140** wenigstens eine Gegenmaßnahme aus. Diese Aktoren können in zwei verschiedenen Teilnetzwerken des Kommunikationsnetzwerks angeordnete sein.

[0097] Es kann vorgesehen sein, das einer der Aktoren mehreren weiteren Aktoren Anweisungen zu der Gegenmaßnahme über das Kommunikationsnetzwerk **100** sendet.

[0098] In einem optionalen Schritt **607** wird die aggregierte Information über erkannte Anomalien von der Aggregationskomponenten an die Kommunikationskomponente gesendet. In einem optionalen Schritt **608** wird Information über eine Reaktion an die von der Reaktionskomponente über eine fünfte Verbindung and die Kommunikationskomponente gesendet.

[0099] Die Kommunikationskomponente stellt eine Schnittstelle dar, die erkannte Anomalien in einem optionalen Schritt **609** insbesondere an ein Backend kommuniziert. Die Kommunikationskomponente kann auch ausgebildet sein, Anweisungen, insbesondere von einem Backend zu empfangen und an die andere Komponente zu senden. Verbindungen im Kommunikationsnetzwerk **100** sind in diesem Falle bidirektional ausgebildet.

[0100] Die Verbindungen erfolgen über das Kommunikationsnetzwerk **100**. Dadurch ist für die Kommunikation keine separate Hardware erforderlich. Es wird beispielsweise Automotive-Ethernet-Netzwerk oder ein Bussystem, wie Controller Area Network (CAN) Bus verwendet.

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 102017210787 [0002]
- DE 102017213119 [0002]

Patentansprüche

1. Verfahren zur Behandlung einer Anomalie in einem Kommunikationsnetzwerk (100), insbesondere eines Kraftfahrzeugs, **dadurch gekennzeichnet**, dass wenigstens ein Detektor (124, 125, 126) einen Datenstrom im Kommunikationsnetzwerk (100) analysiert (601), wobei der wenigstens eine Detektor (124, 125, 126) wenigstens eine Anomalie durch ein regelbasiertes Anomalieerkennungsverfahren erkennt, wenn wenigstens ein Parameter für ein Datenpaket des Datenstroms von einem Sollwert abweicht, wobei der wenigstens eine Detektor (124, 125, 126) Information über wenigstens eine erkannte Anomalie über das Kommunikationsnetzwerk (100) sendet (602, 603).

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, dass wenigstens ein Aktor (135, ..., 140) Information über wenigstens eine vom wenigstens einen Detektor (124, 125, 126) erkannte Anomalie über das Kommunikationsnetzwerk (100) empfängt (603, 605), und wobei der wenigstens eine Aktor (135, ... 140) abhängig von der Information über die wenigstens eine vom wenigstens einen Detektor (124, 125, 126) erkannte Anomalie wenigstens eine Gegenmaßnahme zur Behandlung der Anomalie auslöst (606).

3. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet**, dass wenigstens ein Aggregator (127, ..., 134) Information über wenigstens eine erkannte Anomalie von wenigstens einem Detektor (124, 125, 126) empfängt (602) und wenigstens eine erkannte Anomalie über das Kommunikationsnetzwerk (100) an wenigstens einen Aktor (135, ... 140) sendet (605).

4. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet**, dass wenigstens zwei Detektoren Datenpakete des Datenstroms auf verschiedenen Geräten im Kommunikationsnetzwerk (100) und/oder in demselben Teilnetzwerk analysieren (601).

5. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet**, dass wenigstens zwei, auf unterschiedlichen Geräten im Kommunikationsnetzwerk (100) und/oder auf unterschiedlichen Geräten in zwei verschiedenen Teilnetzwerken des Kommunikationsnetzwerks (100) angeordnete Aktoren wenigstens eine Gegenmaßnahme auslösen (606).

6. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet**, dass wenigstens zwei, auf unterschiedlichen Geräten im Kommunikationsnetzwerk (100) und/oder auf unterschiedlichen Geräten in zwei verschiedenen Teilnetzwerken des Kommunikationsnetzwerks (100) angeordnete Aggregatoren Information über erkannte Anomalien aggregieren (604), wobei ein weiterer Aggregator diese Information über erkannte Anomalien von den wenigstens zwei Aggregatoren aggregiert (604).

7. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet**, dass eine Schnittstelle erkannte Anomalien insbesondere an ein Backend kommuniziert (609) und/oder Anweisungen insbesondere von einem Backend empfängt.

8. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet**, dass der Datenstrom zwischen Steuergeräten innerhalb wenigstens eines Teilnetzwerks des Kommunikationsnetzwerks (100) von einem Detektor analysiert wird, der auf einem dieser Steuergeräte angeordnet ist und/oder dass der Datenstrom zwischen Steuergeräten aus verschiedenen Teilnetzwerken des Kommunikationsnetzwerks (100), die über ein Gateway (101) oder Steuergerät (103, 105) miteinander verbunden sind, von einem Detektor analysiert wird, der auf dem Gateway oder diesem Steuergerät angeordnet ist.

9. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet**, dass wenigstens ein Detektor (125a, 125b; 126a, ..., 126d) und/oder wenigstens ein Aggregator innerhalb wenigstens eines Teilnetzwerks des Kommunikationsnetzwerks verteilt auf mehreren Steuergeräten ausgeführt wird und/oder verteilt auf wenigstens einem Steuergerät und wenigstens einem Gateway (101) ausgeführt wird.

10. Verfahren nach einem der vorherigen Ansprüche, **dadurch gekennzeichnet**, dass einer der Aktoren mehreren weiteren Aktoren Anweisungen zu wenigstens einer Gegenmaßnahme über das Kommunikationsnetzwerk sendet.

11. Computerprogramm, das eingerichtet ist, das Verfahren nach einem der vorherigen Ansprüche auszuführen, wenn es auf einem Computer ausgeführt wird.

12. Maschinenlesbares Speichermedium, auf dem das Computerprogram nach Anspruch 11 gespeichert ist.

13. Vorrichtung zur Behandlung einer Anomalie in einem Kommunikationsnetzwerk, insbesondere eines Kraftfahrzeugs, **dadurch gekennzeichnet**, dass wenigstens ein Detektor (124, 125, 126) eingerichtet ist, einen Datenstrom im Kommunikationsnetzwerk zu analysieren, wobei der wenigstens eine Detektor (124, 125, 126) eingerichtet ist, wenigstens eine Anomalie durch ein regelbasiertes Anomalieerkennungsverfahren zu erkennen, wenn wenigstens ein Parameter für ein Datenpaket des Datenstroms von einem Sollwert abweicht, wobei der wenigstens eine Detektor (124, 125, 126) eingerichtet ist, Information über

wenigstens eine erkannte Anomalie über das Kommunikationsnetzwerk zu senden.

14. Vorrichtung nach Anspruch 13, **dadurch gekennzeichnet**, dass, wobei wenigstens ein Aktor eingerichtet ist, Information über wenigstens eine vom Detektor (124, 125, 126) erkannte Anomalie über das Kommunikationsnetzwerk zu empfangen, und wobei der wenigstens eine Aktor (135, ... 140) eingerichtet ist, abhängig von der Information über die wenigstens eine vom Detektor (124, 125, 126) erkannte Anomalie wenigstens eine Gegenmaßnahme zur Behandlung der Anomalie auszulösen.

15. Vorrichtung nach Anspruch 12 oder 13, **dadurch gekennzeichnet**, dass wenigstens ein Aggregator eingerichtet ist, Information über wenigstens eine erkannte Anomalie von wenigstens einem Detektor (124, 125, 126) zu empfangen und wenigstens eine erkannte Anomalie über das Kommunikationsnetzwerk an wenigstens einen Aktor (135, ... 140) zu senden.

Es folgen 3 Seiten Zeichnungen

Anhängende Zeichnungen

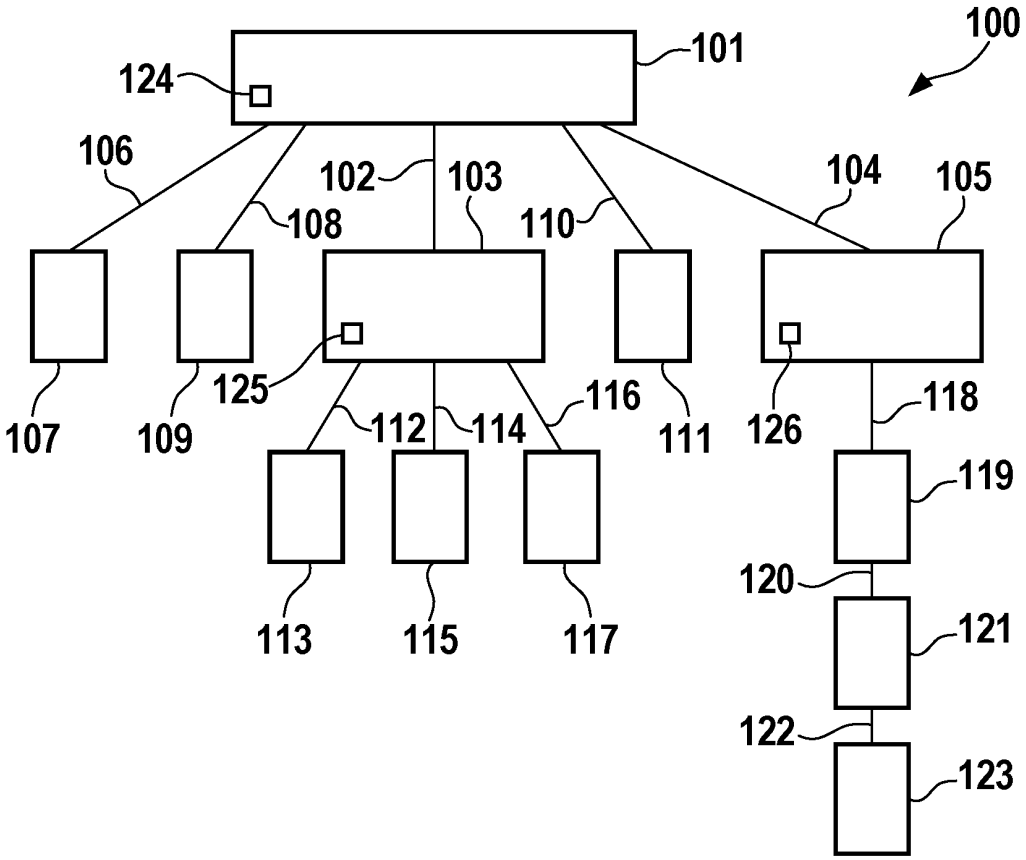


Fig. 1

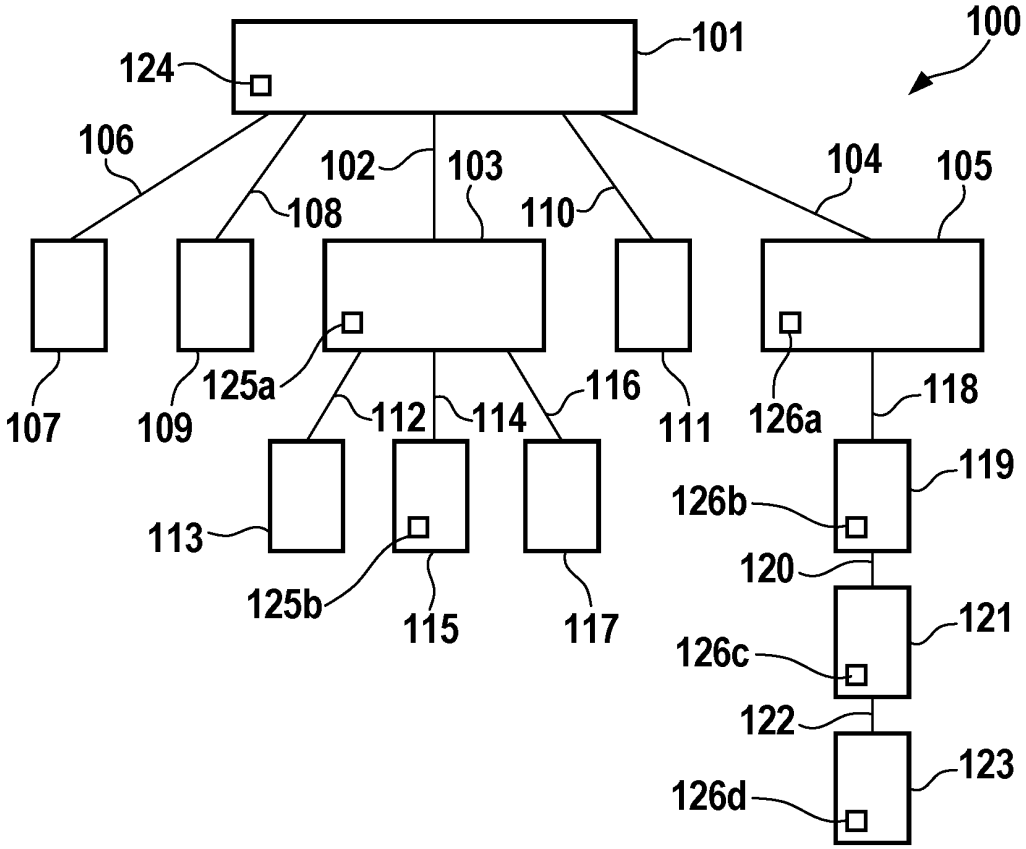


Fig. 2

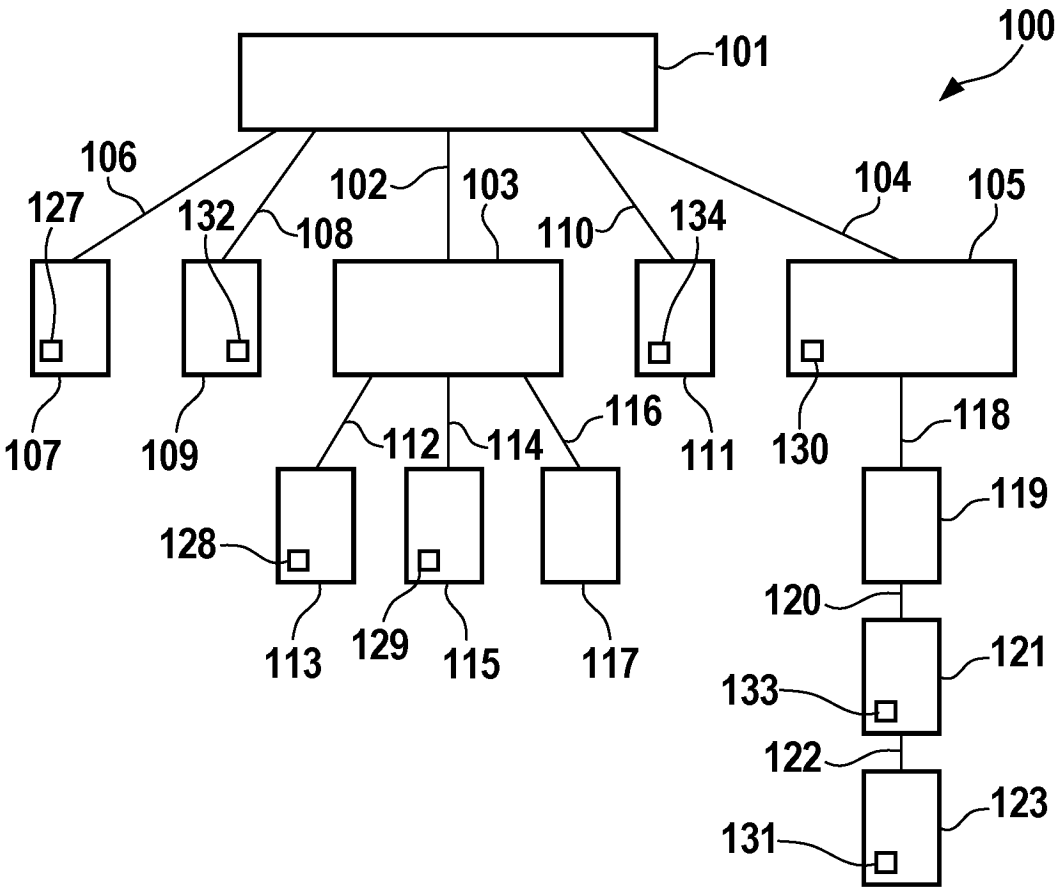

100
101
106
127
132
108
102
103
110
134
104
105
107
109
112
114
116
111
130
118
119
128
120
121
113
129
115
117
133
122
123
131

Fig. 3

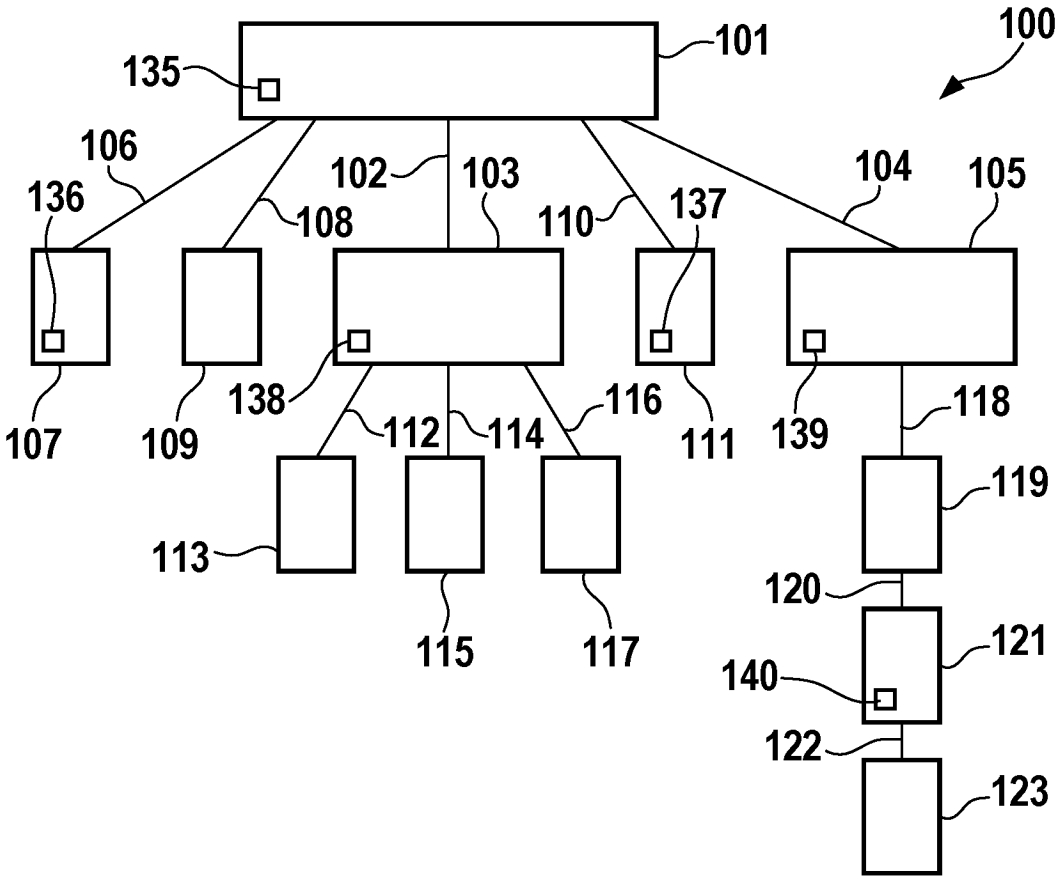

100
101
135
106
136
102
103
108
110
137
104
105
107
109
138
112
114
116
111
139
118
119
113
120
121
115
117
140
122
123

Fig. 4

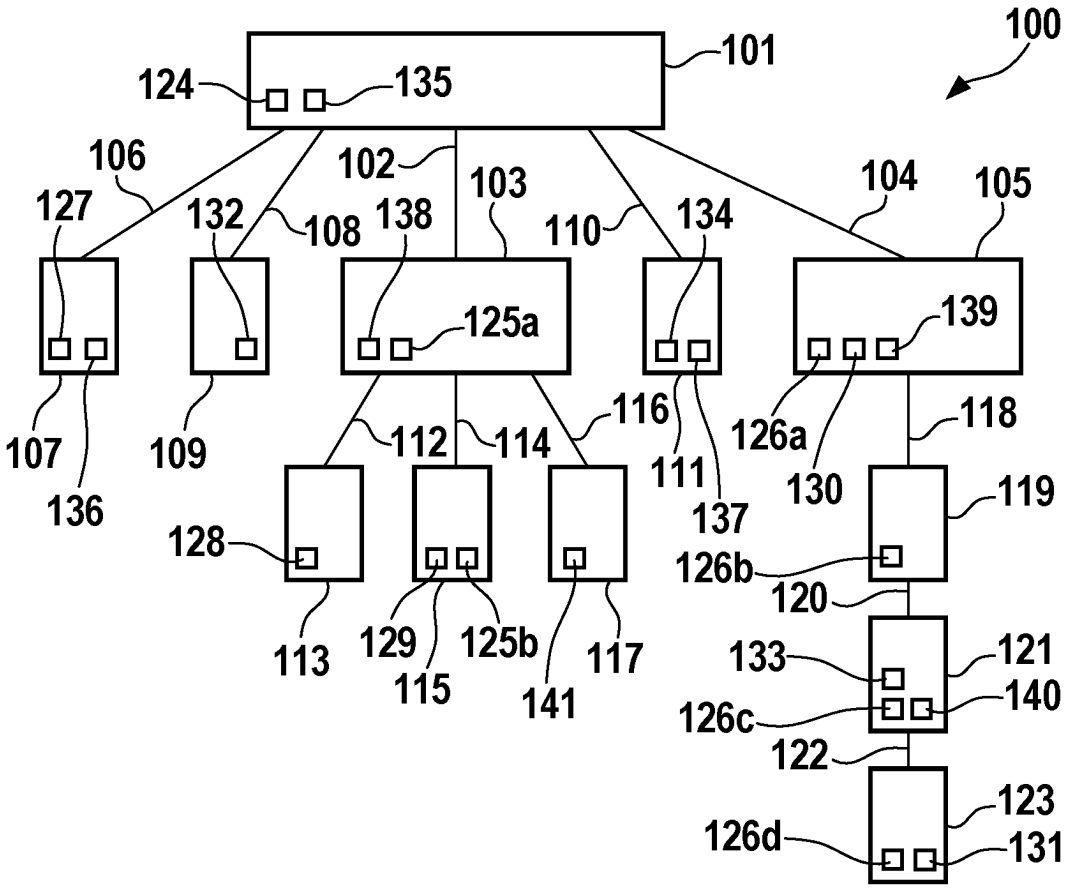

100
101
124
135
106
102
103
104
105
127
132
108
138
110
134
125a
139
107
109
112
114
116
126a
118
136
111
130
119
128
137
126b
120
113
129
125b
117
133
121
115
141
126c
140
122
123
126d
131

Fig. 5

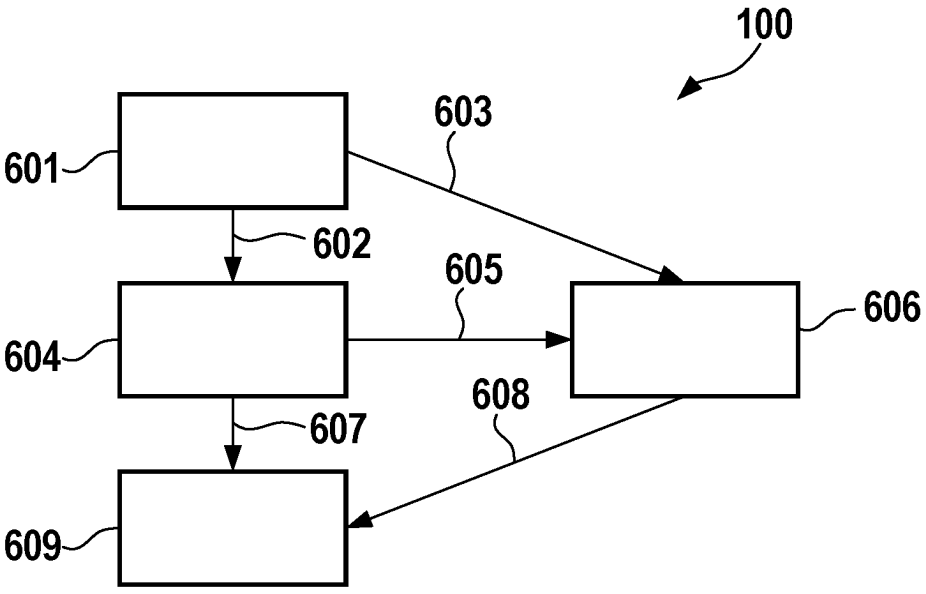

100
603
601
602
605
606
604
608
607
609

Fig. 6