(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
02. November 2017 (02.11.2017)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2017/186457 A1

(51) Internationale Patentklassifikation:
H04L 12/24 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2017/057914

(22) Internationales Anmeldedatum:
04. April 2017 (04.04.2017)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2016 207 423.7
29. April 2016 (29.04.2016) DE

(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Werner-von-Siemens-Straße 1, 80333 München (DE).

(72) Erfinder: **FRANK, Anton**; Ekbertstr. 6, 38122 Braunschweig (DE). **SCHULZ, Oliver**; Lehmkuhlenweg 19, 31234 Edemissen (DE).

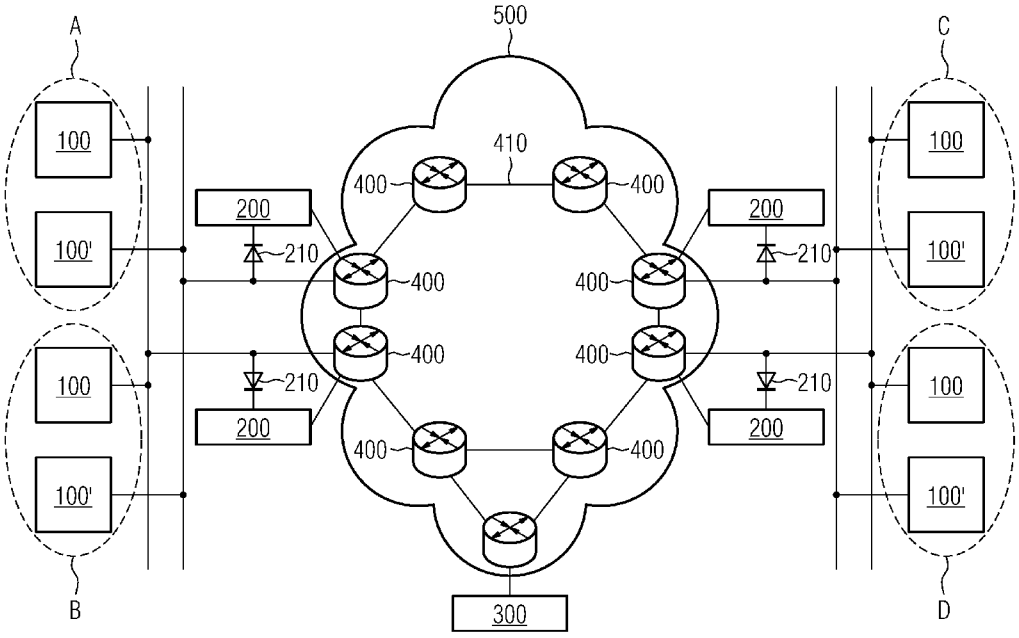
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW,

(54) **Title:** METHOD FOR PATH REDUNDANCY ASSESSMENT IN A BACKBONE NETWORK

(54) **Bezeichnung:** VERFAHREN ZUR WEGREDUNDANZBEWERTUNG IN EINEM BACKBONE-NETZWERK

FIG 1



(57) **Abstract:** The invention relates to a network monitoring unit for path redundancy assessment of communication links in a backbone network (500). The network monitoring unit is designed to receive meta-data, signatures and/or time stamps detected at transfer points, to identify a pair of logically redundant communication links using the meta-data, signatures and/or time stamps, to generate information tables (320, 320') for the identified communication links (AC, AC') by merging said meta-data, signatures and/or time stamps, and to evaluate the information tables (320, 320') with respect to correlation (E4) of the meta-data, signatures and/or time stamps.

(57) **Zusammenfassung:** Eine Netzwerküberwachungseinheit wird beschrieben zur Wegredundanzbewertung von Kommunikationsverbindungen in einem Backbone-Netzwerk (500). Die Netzwerküberwachungseinheit ist ausgebildet, an Übergabepunkten erfasste

[Fortsetzung auf der nächsten Seite]

WO 2017/186457 A1

GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

Metadaten, Signaturen und/oder Zeitstempel zu empfangen und ein Paar logisch redundanter Kommunikationsverbindungen unter Verwendung der Metadaten, Signaturen und/oder Zeitstempel zu identifizieren, Informationstabellen (320, 320') für die identifizierten Kommunikationsverbindungen (AC, AC') durch Zusammenführen der Metadaten, Signaturen und/oder Zeitstempel zu erzeugen und die Informationstabellen (320, 320') bezüglich Korrelation (E4) der Metadaten, Signaturen und/oder Zeitstempel zu evaluieren.

Beschreibung

Verfahren zur Wegredundanzbewertung in einem Backbone-Netzwerk

Die Erfindung betrifft ein Verfahren zur Wegredundanzbewertung von Kommunikationsverbindungen in einem Backbone-Netzwerk. Die Erfindung betrifft weiterhin eine Netzwerküberwachungseinheit und ein System für eine solche Wegredundanzbewertung.

Seit Jahren findet eine zunehmende Vernetzung von Rechnersystemen in industriellen Domänen statt. Zudem werden Übertragungsnetzwerke über größere Distanzen von vielen verschiedenen Anwendungen genutzt, um die Infrastruktur effizient auszulasten. Eine solche Entwicklung lässt sich zum Beispiel im Bahnbereich beobachten, wo vernetzte Stellwerksrechner an verschiedensten Standorten dasselbe Backbone-Netzwerk verwenden, wie auch die Leittechnik, Kundeninformationssysteme und Verwaltungssysteme. Die Dienste haben dabei unterschiedliche Anforderungen an die Datenübertragung in Bezug auf die Dienstqualität (QoS für englisch: Quality of Service).

Bei der Vernetzung von Rechnersystemen mit signaltechnischer Sicherheitsverantwortung überwachen Safety-Protokolle (beispielsweise nach EN50159:2010) den Datenaustausch auf Übertragungsfehler.

Fehler wie zum Beispiel Telegrammverluste, Telegrammverfälschungen, Telegrammverzögerungen etc. müssen innerhalb von bestimmten Zeitanforderungen korrigiert werden. Eine Fehlerkorrektur ist in der Regel durch eine Telegrammwiederholung realisiert und da eine Wiederholung Zeit in Anspruch nimmt, können nur bis zu einem gewissen Maß Übertragungsfehler toleriert werden. Wird diese Grenze überschritten, löst die Verbindungsüberwachung (Safety-Protokoll) eine auf Sicherheit gerichtete Reaktion aus, was für das Gesamtsystem eine Einschränkung der Systemfunktion zur Folge hat. Beispielsweise

bedeutet dies in einem verteilten Stellwerksystem Auswirkungen auf den bahntechnischen Betrieb, da die Automatisierungsfunktion eingeschränkt wird.

Des Weiteren steigt die Bedrohung von verteilten Automatisierungsfunktionen durch Cyber-Angriffe, die aus komplexen Infrastrukturen heraus zunehmend wahrscheinlicher werden. Das Implementieren von Schutzmaßnahmen in der Infrastruktur und in den Teilnehmern ist erforderlich und wird mit der Infrastrukturgröße komplexer. Daher ist neben den schützenden Maßnahmen auch eine Überwachung auf Angriffsversuche zwingend erforderlich.

In Systemen mit signaltechnischer Sicherheitsverantwortung ist die Überwachung der Übertragungseigenschaften von entscheidender Bedeutung, um sowohl ein Degradieren von QoS-Eigenschaften als auch Angriffsversuche zu detektieren. Damit sollen der Infrastrukturadministration Hinweise gegeben werden, bevor es zu einem Verlust der Systemfunktion oder gar einer Manipulation der signaltechnischen Sicherheit kommt. So können rechtzeitig Maßnahmen ergriffen werden. Zudem ist ein Melden von IT-Sicherheitsvorfällen in kritischen Infrastrukturen von dem IT-Sicherheitsgesetz gefordert, was eine gewisse Sensorik voraussetzt. Um höchste Verfügbarkeitsanforderungen zu realisieren, werden redundante Übertragungswege über die Infrastruktur genutzt. Diese sind knoten- und kantendisjunkt ausgelegt, das heißt es werden verschiedene Übertragungswege und verschiedene Netzwerkkomponenten zur Übertragung redundanter Daten verwendet. Ein Einzelfehler wirkt sich damit nur auf einen der beiden redundanten Übertragungswege aus. Ein hochverfügbarer Systemteilnehmer besitzt eine Wegredundanzfunktion, mit welcher z.B. die zu übertragenen Nutzinformationen identisch über mehrere Übertragungswege zum Empfänger versendet werden. Eine solche Übertragungsfunktion ist zum Beispiel als Wegredundanz-Schicht vom Safety-Protokoll RaSTA (DIN VDE V 0831-200) definiert.

Die Infrastruktur für die redundante Übertragung kann auf mehrere Weisen knoten- und kantendisjunkt ausgelegt werden. Es können a) vollständig getrennte Infrastrukturen aufgebaut oder b) knotendisjunkte Zugangspunkte geschaffen werden, die in einer gemeinsamen Infrastruktur redundante Daten durch entsprechende Konfiguration kantendisjunkt übertragen.

Letzteres ist die wirtschaftlichere Variante und mit den heutigen Infrastrukturkomponenten möglich. Liegt eine gemeinsame Infrastruktur für knoten- und kantendisjunkte Übertragung vor, so gibt es neben den bereits veröffentlichten Techniken zur Überwachung von Übertragungseigenschaften (z.B. QoS und Cyber Intrusion Detection) noch die Anforderung, die Eigenschaft „Knoten- und Kantendisjunktheit" sicherzustellen.

Sollten Wege oder Komponenten in der Infrastruktur ausfallen, werden verbleibende Teile so rekonfiguriert, dass möglichst alle logischen Verbindungen von Teilnehmern wieder hergestellt werden können. So ist es möglich, dass die genannte Wegredundanzfunktion von einem Safety-Protokoll (z.B. RaSTA) den Ausfall eines Weges nicht offenbart, da die Infrastruktur einen alternativen Pfad für die Verbindung gewählt hat. Hierbei kann es aber sein, dass dieser Pfad nicht mehr knoten- oder kantendisjunkt zu einer redundanten Übertragung dieses Safety-Protokolls ist.

Als Folge reduziert sich die Verfügbarkeit der signaltechnisch sicheren Funktion, da Einzelfehler in der Infrastruktur nun redundante Verbindungen gleichzeitig betreffen (keine stochastische Unabhängigkeit von Fehlern).

In verteilten Automatisierungssystemen, in denen ein Übertragungsdienst als Bereitstellung genutzt wird, ist es oft schwierig, die Anforderungen an die Datenübertragung mit ihren tatsächlichen Eigenschaften zu vergleichen.

Die Aufgabe besteht darin, ein Verfahren anzugeben, mit dem eine Wegredundanzbewertung von Kommunikationsverbindungen be-

wertet werden kann, sodass Schlüsse auf die Verfügbarkeit der signaltechnischen Funktion oder Wegausfälle möglich sind.

Erfindungsgemäß wird ein Verfahren gemäß Anspruch 1, eine Netzwerküberwachungseinheit gemäß Anspruch 7, eine Datenerfassungseinheit gemäß Anspruch 10 und ein System gemäß Anspruch 11 zur Verfügung gestellt.

Das erfindungsgemäße Verfahren zur Wegredundanzbewertung von zwei logisch redundanten Kommunikationsverbindungen, umfasst: Identifizieren der Kommunikationsverbindungen unter Verwendung von Metadaten von über die Kommunikationsverbindungen übertragenen Datenpaketen, Erzeugen von Informationstabellen für die Kommunikationsverbindungen durch Zusammenführen der Metadaten und Evaluieren der Informationstabellen bezüglich Korrelation der Übertragungseigenschaften.

Die erfindungsgemäß vorgestellte Netzwerküberwachungseinheit ist zur Wegredundanzbewertung von Kommunikationsverbindungen in einem Backbone-Netzwerk ausgebildet. Die Netzwerküberwachungseinheit ist weiterhin ausgebildet, an Übergabepunkten erfasste Metadaten, Signaturen und/oder Zeitstempel zu empfangen und ein Paar logisch redundante Kommunikationsverbindungen unter Verwendung der Metadaten, Signaturen und/oder Zeitstempel zu identifizieren, Informationstabellen für die identifizierten Kommunikationsverbindungen durch Zusammenführen der Metadaten, Signaturen und/oder Zeitstempel zu erzeugen und die Informationstabellen bezüglich Korrelation der Metadaten, Signaturen und/oder Zeitstempel zu evaluieren.

Korrelieren die Übertragungseigenschaften, sind die Wege der Kommunikationsverbindungen nicht stochastisch unabhängig und damit nicht im Sinne der Verfügbarkeit redundant.

In einer bevorzugten Ausführungsform bestehen die Kommunikationsverbindungen teilweise in einem Backbone-Netzwerk zwischen zugehörigen Übergabepunkten des Backbone-Netzwerks und umfassen keinen gemeinsamen Übergabepunkt. Das Verfahren um-

fasst in der bevorzugten Ausführungsform Bestimmen der Übertragungseigenschaften unter Verwendung von Metadaten, Signaturen und/oder Zeitstempeln von über die Kommunikationsverbindungen übertragenen Datenpaketen. Weiterhin kann das Verfahren umfassen: Erfassen der Metadaten, Signaturen und/oder Zeitstempel durch den Übergabepunkten zugeordneten Datenerfassungseinheiten.

So kann in einer bevorzugten Ausführungsform die Bestimmung der Übertragungseigenschaften realisiert werden.

Die erfassten Metadaten, Signaturen und/oder Zeitstempel können an eine Netzwerküberwachungseinheit übertragen werden, die die Wegredundanzbewertung durchführt.

So kann in einer bevorzugten Ausführungsform die Wegredundanzbewertung realisiert werden.

Das Verfahren kann weiterhin umfassen: Vergleichen der bestimmten Korrelation mit mindestens einem Schrankenwert und Bewerten der Wegredundanz anhand des Vergleichsergebnisses oder der Vergleichsergebnisse.

Der Schrankenwert ermöglicht einfach, zwischen ausreichend und nicht ausreichend redundanten Kommunikationsverbindungen zu unterscheiden.

Der Schrankenwert kann ein zuvor bestimmter Korrelationswert sein.

Damit werden Wegausfälle detektierbar.

Die bestimmten Übertragungseigenschaften können Latenzzeitschwankungen und/oder Telegrammbilanzen umfassen.

Dies sind einfach bestimmbare Übertragungseigenschaften.

Die erfindungsgemäß vorgestellte Datenerfassungseinheit ist zur rückwirkungsfreien Datenerfassung ausgebildet und umfasst: ein Mitleseelement zum Mitlesen von Datenpaketen, eine Speichereinheit zum Speichern mitgelesener Datenpakete, eine Datenpaketverarbeitungseinheit zum Bestimmen von Zeitstempeln, von Metadaten und/oder Signaturen der Datenpakete und eine Übertragungseinheit zur Übertragung der bestimmten Zeitstempel, Metadaten und/oder Signaturen an eine Netzwerküberwachungseinheit. Die Datenerfassungseinheit bestimmt die Metadaten durch Telegrammfilter unter Verwendung von Headerinformationen der Datenpakete und/oder die Signaturen unter Verwendung von Prozessdaten sowie eines Zeitstempels, der einen Mitlesezeitpunkt angibt.

Das erfindungsgemäß vorgestellte System zur Wegredundanzbewertung von Kommunikationsverbindungen in einem Backbone-Netzwerk umfasst eine erfindungsgemäße Netzwerküberwachungseinheit und Datenerfassungseinheiten, die den Übergabepunkten des Netzwerks zugeordnet sind, zwischen denen die Kommunikationsverbindungen bestehen.
Die Datenerfassungseinheiten sind gemäß der Erfindung ausgebildet und weiterhin ausgebildet, die Metadaten, Signaturen und Zeitstempel an die Netzwerküberwachungseinheit zu übertragen.

Die oben beschriebenen Eigenschaften, Merkmale und Vorteile dieser Erfindung sowie die Art und Weise, wie diese erreicht werden, werden klarer und deutlicher verständlich im Zusammenhang mit der folgenden Beschreibung der Ausführungsbeispiele, die im Zusammenhang mit den Zeichnungen näher erläutert werden. Es zeigen beispielhaft und schematisch:

Figur 1 eine Vernetzung in einem Backbone-Netzwerk mit einem erfindungsgemäßen System,

Figur 2 eine Datenerfassungseinheit gemäß der Erfindung,

Figur 3 die Datenerfassungseinheit im Detail und

Figur 4 eine Netzwerküberwachungseinheit gemäß der Erfindung.

In der Figur 1 ist eine Vernetzung in einem Backbone-Netzwerk 500 mit einem erfindungsgemäßen System gezeigt.

Das Backbone-Netzwerk 500 umfasst über Kanten 410 verbundene Knoten 400 und eine Netzwerküberwachungseinheit 300, kurz NMU für englisch: Network Monitoring Unit, die mit mindestens einem der Knoten 400 verbunden ist. Das Backbone-Netzwerk 500 verbindet mittels der Knoten 400 Prozessrechner 100 an verschiedenen Standorten A, B, C, D. Einige der Knoten 400 sind dabei als Übergangspunkte zu Standortnetzwerken der jeweiligen Prozessrechner 100 ausgebildet.

Die Prozessrechner 100 sind als redundante und gleichlaufende Rechnerpaare 100, 100‘ an Standorten A, B, C und D ausgebildet. Jeder Rechner eines selben Paars eines Standorts ist mit einem anderen Rechner eines Paars an einem anderen Standort logisch unabhängig verbunden. Es besteht im dargestellten Beispiel eine logische Verbindung von Prozessrechner 100 am Standort A zu Prozessrechner 100 am Standort C und, dazu logisch redundant, eine logische Verbindung von Prozessrechner 100‘ am Standort A zu Prozessrechner 100‘ am Standort C. Entsprechend bestehen im dargestellten Beispiel logische Verbindungen von Prozessrechnern 100, 100‘ am Standort B zu Prozessrechnern 100, 100‘ am Standort D. Die Verbindungen umfassen die Übergabepunkte in beziehungsweise aus dem Backbone-Netzwerk.

Den Übergangspunkten sind Datenerfassungseinheiten 200, kurz DCU für englisch: Data Capture Unit, zugeordnet, die ein passives Mitleseelement 210 umfassen. Das Mitleseelement 210 wird auch als Tap bezeichnet.

Ein Mitleseelement 210 ist eine Hardware-Vorrichtung, die eine Möglichkeit bietet, auf Datenpakete, über die

Übergabepunkte fließen, passiv, also im Sinne der signaltechnischen Sicherheit rückwirkungsfrei, zuzugreifen. Das Mitleseelement im Beispiel umfasst mindestens drei Anschlüsse: einen Eingang 211, einen Ausgang 213 und einen Monitor-Anschluss 212. Datenpakete werden am Eingang 211 empfangen und am Ausgang 213 unverändert ausgegeben. Ein Abgriff ist zwischen Eingang 211 und Ausgang 213 eingefügt, der Kopien der Datenpakete am Monitor-Anschluss 212 zur Verfügung stellt. Andere Komponenten der Datenerfassungseinheiten haben aufgrund der Konstruktion des Taps keine technische Möglichkeit, die originalen Datenbits zu beeinflussen.

Wie in Figuren 2 und 3 gezeigt umfassen die Datenerfassungseinheiten 200 weiterhin eine Speichereinheit 220 und Einheiten 230, 240, 250 zur Bestimmung von Signaturen (SG), Metadaten (MD) und Zeitstempeln (TS). Bestimmte (SG), Metadaten (MD) und Zeitstempeln (TS) werden über einen Ausgang 260, der mit dem Backbone-Netzwerk 500 verbunden ist, an die Netzwerküberwachungseinheit 300 übertragen.

Die Einheiten 230, 240, 250 können durch eine einzige Datenverarbeitungseinheit realisiert sein.

Die Einheit 250 fügt Datenpaketen einen Zeitstempel TS zu.

Die Einheit 240 ist beispielsweise ein Telegrammfilter der Headerinformationen IP, TH der Datenpakete verwendet, um Telegrammverlust und Telegrammeinfügung zu erkennen. Die Einheit 240 ist in Figur 3 beispielhaft ausgebildet, die IP Header- und Transportheader Informationen IP, TH durch die Metadaten MD zu ersetzen, wobei die Metadaten MD Telegrammverlust oder Telegrammeinfügung bezogen sind.

Die Einheit 230 bestimmt die Signaturen SG beispielsweise unter Verwendung von Prozessdaten PD der Datenpakete. Die Einheit 230 ist in Figur 3 beispielhaft ausgebildet, die Prozessdaten PD durch die Signatur SG zu ersetzen.

Die Datenerfassungseinheit 200 entfernt in einem Ausführungsbeispiel aus den Datenpaketen auch einen Ethernet Header EH und einen zyklischen Redundanzprüfwert CRC.

Das rückwirkungsfreie Mitlesen von Datentelegrammen hat den Vorteil, dass für signaltechnisch sichere Datenübertragungen keine besonderen Betrachtungen in der Sicherheitsnachweisführung erbracht werden müssen.

Figur 4 zeigt eine Netzwerküberwachungseinheit 300 gemäß einem Ausführungsbeispiel der Erfindung. Die Netzwerküberwachungseinheit 300 identifiziert in Schritt S1 Kommunikationsverbindungen AC, AC‘ zwischen redundanten Rechnerpaaren 100, 100‘ an Standorten A, C. Dies kann beispielsweise unter Verwendung der Übertragungseigenschaften und/oder Kenntnis über die Kommunikationsverbindungen AC, AC‘ erfolgen. Dann erzeugt die Netzwerküberwachungseinheit 300 in Schritt S2 für jede der Verbindungen AC, AC‘ eine Informationstabelle 320 durch Zusammenführen der Zeitstempel TS, Metadaten MD und/oder Signaturen SG. Die Informationstabellen 320, 320‘ werden in Schritt E4 auf eine Korrelation E4 der Verbindungen hin ausgewertet. Weiterhin kann aus der Informationstabelle 320 Paketverlust E1, E1‘, Paketeinfügung E2, E2‘ und Verbindungsverzögerung E3, E3‘ der Verbindungen AC, AC‘ bestimmt werden.

Das Abbilden von Nutzdaten eines Datenpakets auf Zeitstempel, Metainformationen und/oder Signatur steigert die Effizienz bei der Auswertung von Übertragungseigenschaften. Es wird eine nur sehr geringe Bandbreite zwischen Datenerfassungseinheiten und Netzwerküberwachungseinheit benötigt und die Suche nach Metainformationen eines übertragenen Datenpakets in der Netzwerküberwachungseinheit wird beschleunigt.

In Figur 1 wird eine Systemfunktion durch ein redundantes und gleichlaufendes Rechnerpaar 100, 100‘ an einem Standort A realisiert, welches je eine Verbindung zu einem anderen redundanten Rechnerpaar 100, 100‘ an einem anderen Standort C hält. Hierbei bestehen eine Verbindung von Prozessrechner 100

am Standort A zu Prozessrechner 100 am Standort C und eine dazu redundante Verbindung, über die identische Nutzdaten übertragen werden, von Prozessrechner 100‘ am Standort A zu Prozessrechner 100‘ am Standort C. Es ist jeweils ein redundantes lokales Netzwerk an den beiden Standorten A, C der redundanten Rechner 100, 100‘ vorhanden. Die Standorte A, C sind über das Backbone-Netzwerk 500 miteinander verbunden, welches über disjunkte Übergangspunkte jedes der beiden redundanten lokalen Netzwerke an den Standorten A, C miteinander verbindet. Per Konfiguration wird sichergestellt, dass innerhalb des Backbone-Netzwerks 500 die Daten der redundanten lokalen Netzwerke knoten- und kantendisjunkt übertragen werden.

Dadurch ergeben sich auf unterschiedlichen Teilwegen im Backbone-Netzwerk 500 verschiedene Schwankungen in der Latenzzeit, die durch unterschiedliche Auslastungen hervorgerufen werden.

Die Datenerfassungseinheit 200 können so konfiguriert sein, dass sie bestimmte oder jedes Datenpaket einer Rechnerverbindung mit Zeitstempeln und Metadaten (z.B. Time to Live, Datenlänge, Quell- und Zieladresse) erfassen und über die zugehörigen Nutzdaten eine Signatur bilden. Dieser Vorgang findet auf beiden Seiten des zu überwachenden Backbone-Netzwerkes 500 statt.

Jedes zu erfassende Datenpaket wird folglich zweimal, beim Eintritt und beim Austritt aus dem Backbone-Netzwerk 500, registriert. Die Netzwerküberwachungseinheit 300 übernimmt die Weiterverarbeitung aller mitgelesenen Daten (jeweils bestehend aus Zeitstempel des Lesezeitpunkts, Metainformationen und/oder Signatur der Nutzdaten). In der Netzwerküberwachungseinheit 300 findet eine Bewertung der Übertragungseigenschaften statt.

Für jede logische Verbindung zwischen zwei Prozessrechnern 100 beziehungsweise 100‘ werden in der Netzwerküberwachungs-

einheit 300 mindestens eine, bevorzugt zwei, noch bevorzugter drei oder mehr der folgenden Funktionen/Bewertungen ausgeführt, welche wesentliche Übertragungseigenschaften und mögliche Schwachstellen des zugrunde liegenden Backbone-Netzwerkes 500 offenbaren:

Die Differenz der Zeitstempel (Zeitpunkt des Durchlaufens eines Mitlesepunktes) ist die Latenzzeit zwischen den Mitlesepunkten (und im oben genannten Beispiel die Latenz des Backbone-Netzwerks). Die Differenz der Latenz zu einem Folgepaket ergibt die Latenzzeitschwankung (Jitter).

Gibt es, innerhalb eines vorbestimmten Zeitrahmens, zur Signatur von der Datenerfassungseinheit am Übergabepunkt in das Backbone-Netzwerk keine Entsprechung der Datenerfassungseinheit am Übergabepunkt aus dem Backbone-Netzwerk, so handelt es sich um einen Übertragungsfehler zwischen den Datenerfassungseinheiten, der auch als Telegrammverlust bezeichnet wird und die Dienstqualität (QoS) betrifft. Die Telegrammbilanz ist negativ.

Gibt es zu einer am Übergabepunkt aus dem Backbone-Netzwerk bestimmten Signatur keine innerhalb des vorbestimmten Zeitrahmens am Übergabepunkt in das Backbone-Netzwerk bestimmte, passende Signatur, so handelt es sich um ein Datenpaket, welches nicht aus den überwachten lokalen Netzwerken stammt. Dies wird auch als Telegrammeinfügung bezeichnet. Die Telegrammbilanz ist positiv. Wenn die Teilnetze lückenlos überwacht werden und keine Datenpakete außerhalb der Überwachung stammen dürfen, deutet dieses auf einen Eindringungsversuch (Intrusion) hin.

Wenn es bei den Fehlern in der Telegrammbilanz durch Telegrammeinfügung und Telegrammverlust einen zeitlich engen Zusammenhang gibt, werden Pakete bei ihrer Übertragung scheinbar verfälscht. Hierbei handelt es sich potentiell um einen Angriff.

Wenn ein redundanter Datenstrom mit identischen Nutzdaten existiert, kann eine weitere Bewertung der Übertragungseigenschaften realisiert werden: Die Korrelation der Übertragungseigenschaften der beiden redundanten Datenströme.

Sofern es sich um eine knoten- und kantendiskunkte Übertragung handelt, ist die Korrelation (z.B. der Latenzzeit) gering. Wenn das Backbone-Netzwerk aufgrund einer Rekonfiguration die Datenströme aber über gemeinsame Knoten oder Kanten führt, steigt die Korrelation deutlich, weil sich die Einflüsse des Netzwerkes auf beide Datenströme gleich auswirken.

Die Auslastung des Backbone-Netzwerks schwankt typischerweise, da viele Übertragungen von Daten im Netzwerk stattfinden. Betrifft die Auslastungsschwankung die redundanten Datenverbindungen in korrelierter Weise, kann dies von der Netzwerküberwachungseinheit unabhängig von einem Netzwerkmanagement des Backbone-Netzwerks festgestellt, protokolliert und/oder gemeldet werden.

Die Korrelation der Übertragungseigenschaften ist ein Index für die stochastische Unabhängigkeit der Verbindungen. Eine hohe Korrelation deutet auf geringe stochastische Unabhängigkeit hin, eine geringe Korrelation auf stochastisch unabhängige Verbindungen. Da die stochastische Unabhängigkeit von logischen Verbindungen ein notwendiges Kriterium zur Steigerung von Zuverlässigkeit/Verfügbarkeit beim Nutzen von Redundanz ist und Aufgrund von Backbone-Netzwerktechnologien diese Eigenschaft verletzt werden kann, ist ein Überwachen sinnvoll und vorteilhaft.

Die Erfindung bezieht sich auf die Gesamtarchitektur zum Überwachen eines Backbone-Netzwerks auf bestimmte Übertragungseigenschaften, Systemkomponenten und zugehörige Verfahren. Speziell das erfindungsgemäße Verfahren zur Wegredundanzbewertung bietet Verbesserung bei Netzwerkdiagnose zur Überwachung auf korrelierte Datenströme, die aus Verfügbar-

keitsanforderungen heraus stochastisch unabhängig voneinander sein sollen.

Die Anwendung der Kreuzkorrelationsfunktion auf die Übertragungseigenschaften zweier redundanter, logischer Datenströme setzt diese direkt in Verbindung. Daraus wird ein Mehrwert und Informationsgewinn generiert, der sich nicht aus der Betrachtung der Einzelverbindungen ergibt.

Mit Hilfe des erfindungsgemäßen Verfahrens ist ein Rückschluss auf Eigenschaften und die Konfiguration des zugrunde liegenden Übertragungsnetzwerkes möglich.

Es können mithilfe der Eigenschaften einer Datenverbindung, unabhängig von den Diagnosemöglichkeiten der Teilnehmer, erhöhte Fehlerwahrscheinlichkeit und IT-Security Angriffe offenbart werden.

Ein Aspekt dieser Erfindung liegt im Bewerten der Korrelation von redundanten Datenströmen über ein Übertragungsnetzwerk. Redundante Datenübertragungen müssen zur Steigerung der Verfügbarkeit knoten- und kantendisjunkt erfolgen.

Obwohl die Erfindung im Detail durch bevorzugte Ausführungsbeispiele näher illustriert und beschrieben wurde, so ist die Erfindung nicht durch die offenbarten Beispiele eingeschränkt und andere Variationen können vom Fachmann hieraus abgeleitet werden, ohne den Schutzumfang der Erfindung zu verlassen.

Bezugszeichenliste

100, 100‘	Prozessrechnerpaar
200	Datenerfassungseinheit
210	Tap
211	Eingang
212	Monitor-Anschluss
213	Ausgang des Tap
220	Speichereinheit
230	Signaturbestimmungseinheit
240	Paketfiltereinheit
250	Zeitstempeleinheit
260	Ausgang der Datenerfassungseinheit
300	Netzwerküberwachungseinheit
310	Speichereinheit
320, 320‘	Informationstabellen
400	Knoten des Backbone-Netzwerks
410	Kanten
500	Backbone-Netzwerk
A,B,C,D	Standorte
TS	Zeitstempel
SG	Signatur
MD	Metadaten
IP	IP Header
TH	Transportheader
PD	Prozessdaten
CRC	zyklische Kontrollsumme
EH	Ethernet Header
AC, AC‘	Verbindungen zwischen Standorten A und C
S1	Verbindungsidentifikation
S2	Informationstabellenerzeugung
S3	Evaluation
E1, E1‘	Paketverlust
E2, E2‘	Paketeinfügung
E3, E3‘	Verbindungsverzögerung
E4	Verbindungskorrelation

Patentansprüche

1. Verfahren zur Wegredundanzbewertung von zwei logisch redundanten Kommunikationsverbindungen (AC, AC‘), umfassend: Identifizieren (S1) der Kommunikationsverbindungen unter Verwendung von Metadaten von über die Kommunikationsverbindungen (AC, AC‘) übertragenen Datenpaketen, Erzeugen (S2) von Informationstabellen (320, 320‘) für die Kommunikationsverbindungen (AC, AC‘) durch Zusammenführen der Metadaten und Evaluieren der Informationstabellen (320, 320‘) bezüglich Korrelation (E4) der Übertragungseigenschaften.

2. Verfahren nach Anspruch 1, wobei die Kommunikationsverbindungen (AC, AC‘) zumindest teilweise in einem Backbone-Netzwerk (500) zwischen zugehörigen Übergabepunkten des Backbone-Netzwerks (500) bestehen und keinen gemeinsamen Übergabepunkt umfassen, wobei Bestimmen der Übertragungseigenschaften unter Verwendung von Metadaten (MD), Signaturen (SG) und/oder Zeitstempeln (TS) der Datenpakete erfolgt und das Verfahren weiterhin umfasst: Erfassen der Metadaten (MD), Signaturen (SG) und/oder Zeitstempel (TS) durch den zugehörigen Übergabepunkten zugeordnete Datenerfassungseinheiten (200).

3. Verfahren nach Anspruch 2, weiterhin umfassend: Übertragen der erfassten Metadaten (MD), Signaturen (SG) und/oder Zeitstempel (TS) an eine Netzwerküberwachungseinheit (300), die die Wegredundanzbewertung durchführt.

4. Verfahren nach einem der vorangehenden Ansprüche, weiterhin umfassend: Vergleichen der bestimmten Korrelation mit mindestens einem Schrankenwert und Bewerten der Wegredundanz anhand des Vergleichsergebnisses oder der Vergleichsergebnisse.

5. Verfahren nach Anspruch 4, wobei der Schrankenwert ein zuvor bestimmter Korrelationswert ist.

6. Verfahren nach einem der vorangehenden Ansprüche, wobei die bestimmten Übertragungseigenschaften Latenzzeitschwankungen und/oder Telegrammbilanzen umfassen.

7. Netzwerküberwachungseinheit (300) zur Wegredundanzbewertung von Kommunikationsverbindungen, wobei die Netzwerküberwachungseinheit (300) ausgebildet ist, an Übergabepunkten erfasste Metadaten (MD), Signaturen (SG) und/oder Zeitstempel (TS) zu empfangen und ein Paar logisch redundanter Kommunikationsverbindungen unter Verwendung der Metadaten (MD), Signaturen (SG) und/oder Zeitstempel (TS) zu identifizieren, Informationstabellen (320, 320‘) für die identifizierten Kommunikationsverbindungen (AC, AC‘) durch Zusammenführen der Metadaten (MD), Signaturen (SG) und/oder Zeitstempel (TS) zu erzeugen und die Informationstabellen (320, 320‘) bezüglich Korrelation (E4) der Metadaten (MD), Signaturen (SG) und/oder Zeitstempel (TS) zu evaluieren.

8. Netzwerküberwachungseinheit (300) nach Anspruch 7, wobei die Kommunikationsverbindungen zumindest teilweise in einem Backbone-Netzwerk (500) mit Übergabepunkten zu anderen Netzwerken bestehen, das Paar logisch redundanter Kommunikationsverbindungen zwischen zugehörigen Übergabepunkten des Backbone-Netzwerks (500) besteht und keinen gemeinsamen Übergabepunkt umfasst.

9. Netzwerküberwachungseinheit (300) nach Anspruch 7 oder 8, wobei die Netzwerküberwachungseinheit (300) ausgebildet ist, ein Verfahren gemäß einem der Ansprüche 4 bis 6 durchzuführen.

10. Datenerfassungseinheit (200) zur rückwirkungsfreien Datenerfassung umfassend: ein Mitleseelement (210) zum Mitlesen von Datenpaketen, eine Speichereinheit (220) zum Speichern mitgelesener Datenpakete, eine Datenpaketverarbeitungseinheit (230, 240, 250) zum Bestimmen von Zeitstempeln (TS), von Metadaten (MD) und/oder von Signaturen (SG) der Datenpakete und eine Übertragungseinheit zur Übertragung der bestimmten

Zeitstempel (TS), Metadaten (MD) und/oder Signaturen (SG) an eine Netzwerküberwachungseinheit (300), wobei die Metadaten (MD) durch Telegrammfilter (240) unter Verwendung von Headerinformationen (IP, TH) der Datenpakete und/oder die Signaturen (SG) unter Verwendung von Prozessdaten (PD) sowie TS (250) unter Verwendung eines Zeitstempels, der einen Mitlesezeitpunkt angibt, bestimmt werden.

11. System zur Wegredundanzbewertung von Kommunikationsverbindungen in einem Backbone-Netzwerk (500) mit einer Netzwerküberwachungseinheit (300) nach einem der Ansprüche 7 bis 9 und gemäß Anspruch 10, die den Übergabepunkten des Backbone-Netzwerks (500) zugeordnet sind, zwischen denen die Kommunikationsverbindungen bestehen, wobei die Datenerfassungseinheiten (200) ausgebildet sind, die Metadaten (MD), Signaturen (SG) und/oder Zeitstempel (TS) an die Netzwerküberwachungseinheit zu übertragen.

FIG 1

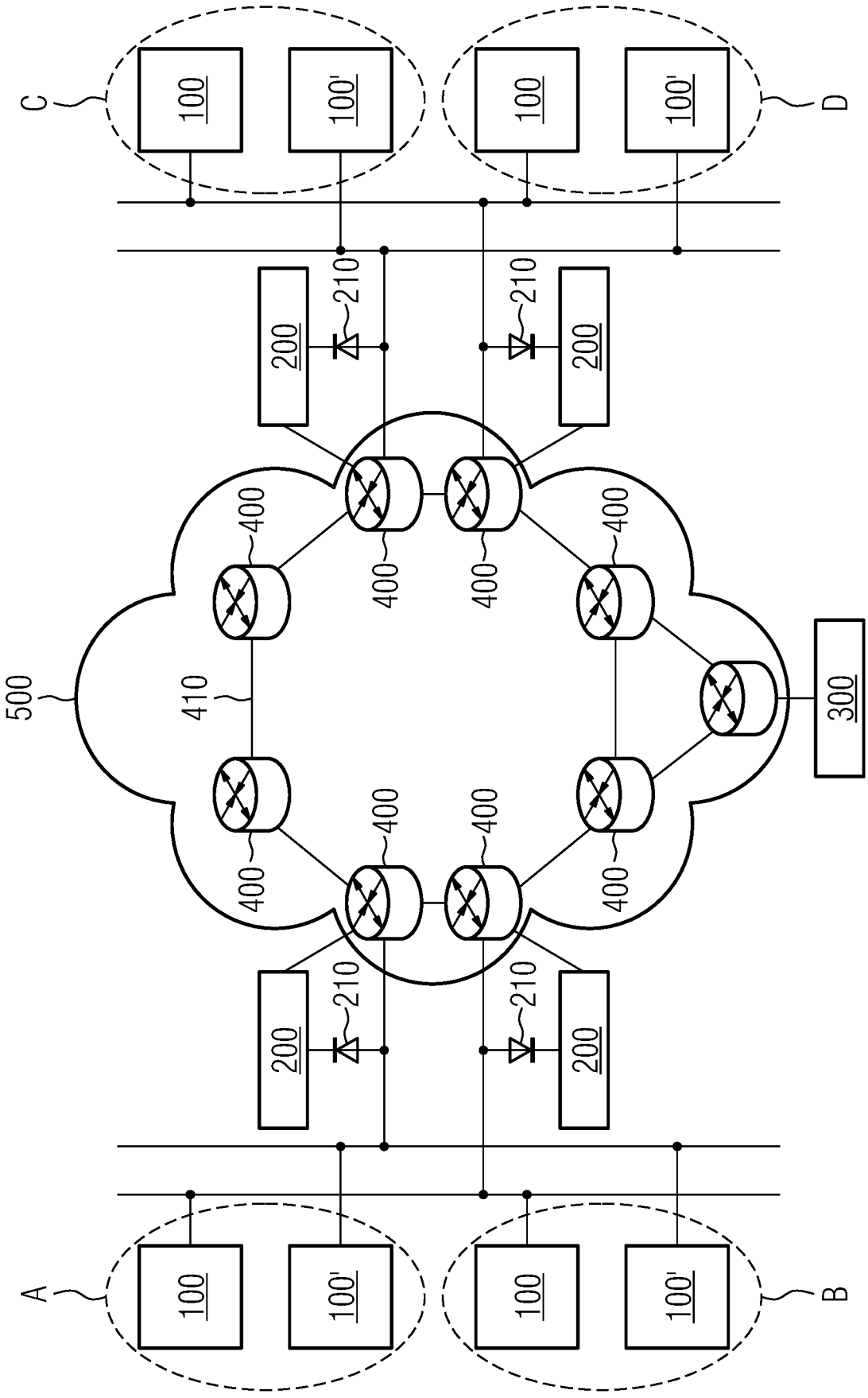


FIG 2

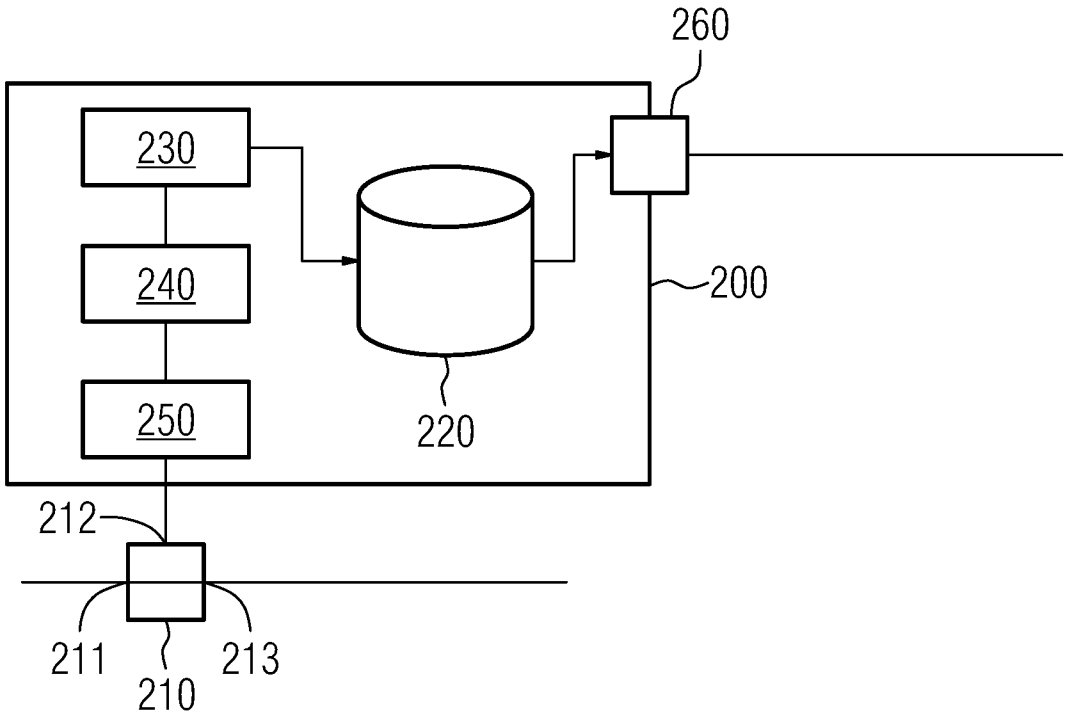

260
230
240
250
220
200
212
211
210
213

FIG 3

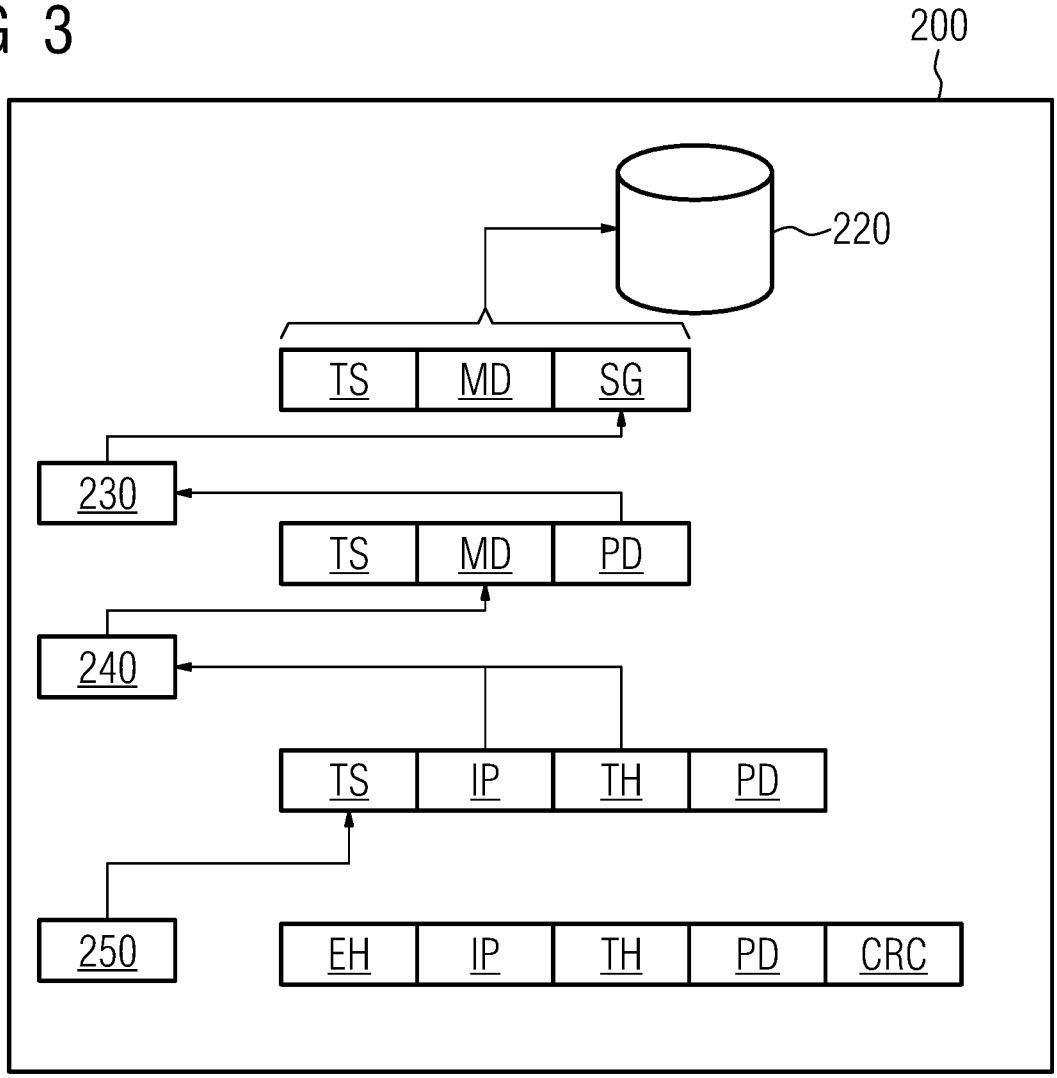
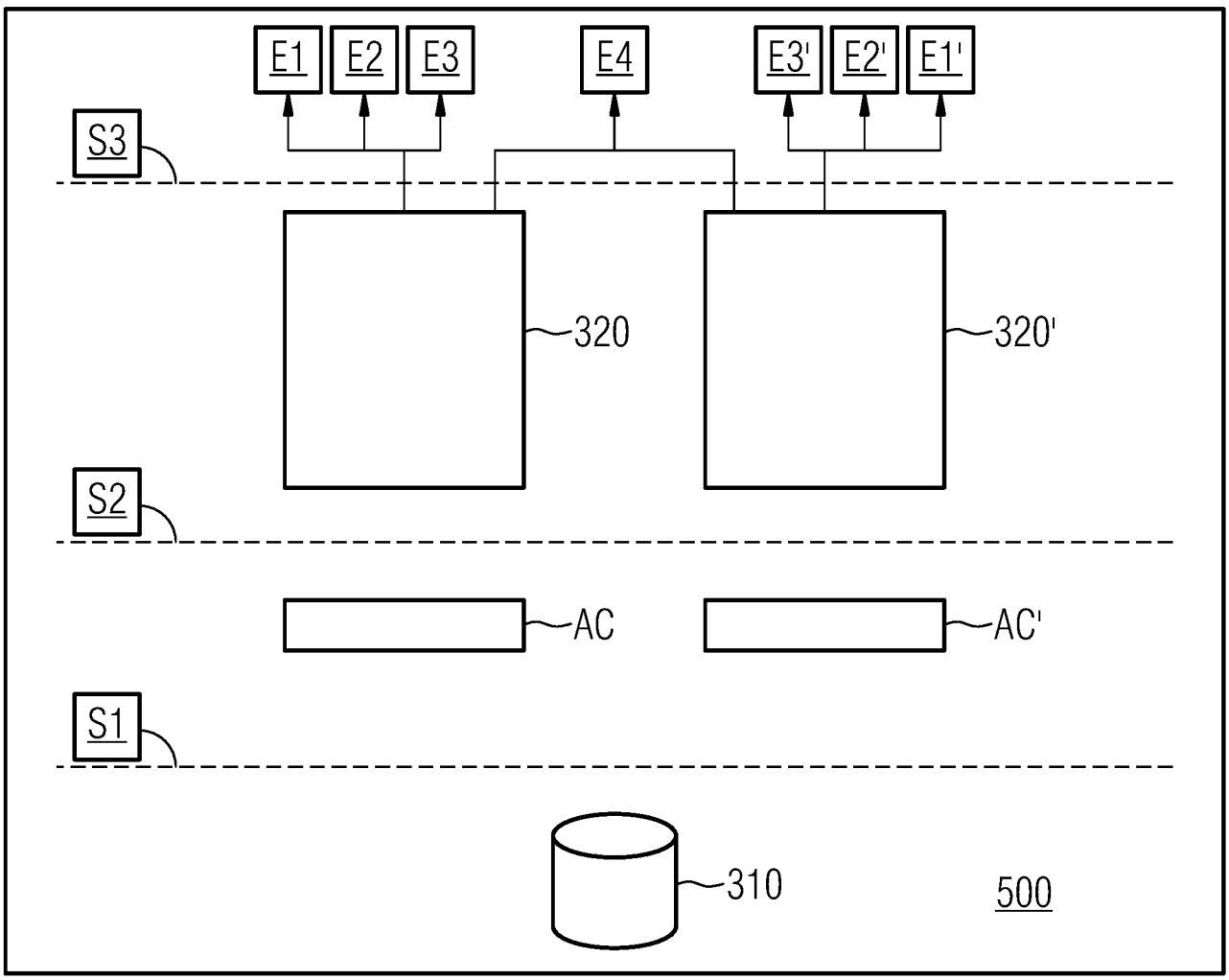

200
220
TS
MD
SG
230
TS
MD
PD
240
TS
IP
TH
PD
250
EH
IP
TH
PD
CRC

FIG 4



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/057914

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/24
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WEIDONG CUI ET AL: "Backup path allocation based on a correlated link failure probability model in overlay networks", NETWORK PROTOCOLS, 2002. PROCEEDINGS. 10TH IEEE INTERNATIONAL CONFEREN CE ON NOV. 12-15, 2002, PISCATAWAY, NJ, USA,IEEE, 12 November 2002 (2002-11-12), pages 236-245, XP010632591, ISBN: 978-0-7695-1856-5 abstract; figure 1 Abschnitt 3 ----- -/--	1-11

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 May 2017	08/06/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Hanigk, Sebastian

2

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	HU BO ET AL: "MLCS: A multi-level correlation scheduling algorithm for multipath transport", 2016 INTERNATIONAL CONFERENCE ON INFORMATION NETWORKING (ICOIN), IEEE, 13 January 2016 (2016-01-13), pages 166-171, XP032877407, DOI: 10.1109/ICOIN.2016.7427108 [retrieved on 2016-03-07] Abschnitt III.B	1-11
A	EP 1 130 850 A2 (TEKTRONIX INC [US]) 5 September 2001 (2001-09-05) abstract; figure 1 paragraph [0012] - paragraph [0018]	1-11

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2017/057914

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1130850 A2	05-09-2001	CN 1324162 A	28-11-2001
		DE 60124970 T2	20-09-2007
		EP 1130850 A2	05-09-2001
		JP 3851097 B2	29-11-2006
		JP 2001268131 A	28-09-2001
		US 6738349 B1	18-05-2004

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2017/057914

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L12/24
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WEIDONG CUI ET AL: "Backup path allocation based on a correlated link failure probability model in overlay networks", NETWORK PROTOCOLS, 2002. PROCEEDINGS. 10TH IEEE INTERNATIONAL CONFEREN CE ON NOV. 12-15, 2002, PISCATAWAY, NJ, USA,IEEE, 12. November 2002 (2002-11-12), Seiten 236-245, XP010632591, ISBN: 978-0-7695-1856-5 Zusammenfassung; Abbildung 1 Abschnitt 3 ----- -/--	1-11

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
31. Mai 2017	08/06/2017

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Hanigk, Sebastian

2

Formblatt PCT/ISA/210 (Blatt 2) (April 2005)

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	HU BO ET AL: "MLCS: A multi-level correlation scheduling algorithm for multipath transport", 2016 INTERNATIONAL CONFERENCE ON INFORMATION NETWORKING (ICOIN), IEEE, 13. Januar 2016 (2016-01-13), Seiten 166-171, XP032877407, DOI: 10.1109/ICOIN.2016.7427108 [gefunden am 2016-03-07] Abschnitt III.B -----	1-11
A	EP 1 130 850 A2 (TEKTRONIX INC [US]) 5. September 2001 (2001-09-05) Zusammenfassung; Abbildung 1 Absatz [0012] - Absatz [0018] -----	1-11

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2017/057914

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 1130850 A2	05-09-2001	CN 1324162 A	28-11-2001
		DE 60124970 T2	20-09-2007
		EP 1130850 A2	05-09-2001
		JP 3851097 B2	29-11-2006
		JP 2001268131 A	28-09-2001
		US 6738349 B1	18-05-2004