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

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

PCT

(43) Internationales Veröffentlichungsdatum
29. November 2007 (29.11.2007)

(10) Internationale Veröffentlichungsnummer
WO 2007/135145 A2

(51) Internationale Patentklassifikation:
Nicht klassifiziert

(21) Internationales Aktenzeichen: PCT/EP2007/054934

(22) Internationales Anmeldedatum:
22. Mai 2007 (22.05.2007)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2006 024 008.1 22. Mai 2006 (22.05.2006) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **NOKIA SIEMENS NETWORKS GMBH & CO. KG** [DE/DE]; St. Martin Str. 76, 81541 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **BUSSER, Jens-Uwe** [DE/DE]; Gustav-Heinemann-Ring 98, 81739 München (DE). **KISS, Adam** [HU/HU]; Halasi 19, H-6000 Keczkemet (HU).

(74) Gemeinsamer Vertreter: **NOKIA SIEMENS NETWORKS GMBH & CO. KG**; Postfach 80 17 60, 81617 München (DE).

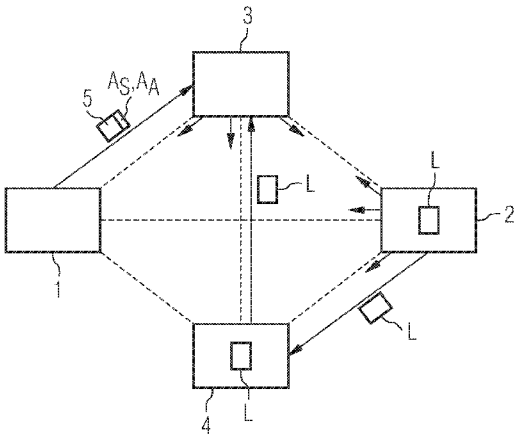
(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC,

[Fortsetzung auf der nächsten Seite]

(54) **Title:** METHOD FOR GENERATION OF A USER-SPECIFIC TRANSMISSION EXCLUSION LIST AND METHOD FOR FORWARDING MESSAGES IN A DECENTRALISED COMMUNICATION SYSTEM

(54) **Bezeichnung:** VERFAHREN ZUM ERSTELLEN EINER TEILNEHMERSPEZIFISCHEN SENDERAUSSCHLUSSLISTE UND VERFAHREN ZUM WEITERLEITEN VON NACHRICHTEN IN EINEM DEZENTRALEN KOMMUNIKATIONSSYSTEM



(57) **Abstract:** At least one transmitter for exclusion is described by giving at least one piece of address information about the transmitter in order to generate a user-specific transmitter exclusion list (L). For each given piece of address information, an irreversible unambiguous representation is generated, deposited in a first list (L1), stored in the decentralised communication system as a user-specific transmitter exclusion list (L). In order to forward messages, a message (5) from a transmitter (1) with provided address information (AS) for forwarding to an addressee (2) is received. The transmitter exclusion list specific to the addressee (2) is read from the decentralised communication system. An irreversible unambiguous representation of the address information of the transmitter is generated and compared with the entries in the user-specific transmitter exclusion list that has been read. Should the irreversible unambiguous representation of the address information of the transmitter not correspond with any of the entries in the user-specific exclusion list, the message is forwarded to the addressee.

[Fortsetzung auf der nächsten Seite]

WO 2007/135145 A2

MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Zum Erstellen einer teilnehmerspezifischen Senderauschlussliste (L) für ein dezentrales Kommunikationssystem wird mindestens ein auszuschließender Sender durch Vorgabe von mindestens einer dem Sender zugeordneten Adressinformation angegeben. Zu jeder der vorgegebenen Adressinformationen wird eine unumkehrbar eindeutige Repräsentation erstellt, die in einer ersten Liste (L1) abgelegt wird. Diese wird als teilnehmerspezifische Senderauschlussliste (L) in dem dezentralen Kommunikationssystem gespeichert. Zum Weiterleiten von Nachrichten wird eine Nachricht (5) eines Senders (1) mit zugeordneten Adressinformation (AS) zur Weiterleitung an einen Adressat (2) entgegengenommen. Die für den Adressat (2) spezifische Senderauschlussliste wird aus dem dezentralen Kommunikationssystem eingelesen. Zu der Adressinformation des Senders wird eine unumkehrbar eindeutige Repräsentation erstellt und diese mit den Einträgen der eingelesenen teilnehmerspezifischen Senderauschlussliste verglichen. Falls die unumkehrbar eindeutige Repräsentation der Adressinformation des Senders keinem der Einträge der teilnehmerspezifischen Senderauschlussliste entspricht, wird die Nachricht an den Adressat weitergeleitet.

Beschreibung

Verfahren zum Erstellen einer teilnehmerspezifischen Senderausschlussliste und Verfahren zum Weiterleiten von Nachrichten in einem dezentralen Kommunikationssystem

Die Erfindung betrifft ein Verfahren zum Erstellen einer teilnehmerspezifischen Senderausschlussliste sowie ein Verfahren zum Weiterleiten einer Nachricht in einem dezentralen Kommunikationssystem. Die Erfindung betrifft weiterhin ein Computerprogrammprodukt, das zur Durchführung der Verfahren geeignet ist.

Als Kommunikationssystem wird eine Netzwerkanordnung mit mindestens zwei Teilnehmergeräten bezeichnet, bei dem Teilnehmer über die Teilnehmergeräte Nachrichten austauschen können. Nachrichten sind in diesem Zusammenhang sowohl textbasierte Meldungen, zum Beispiel SMS (Short Messenger Service), IM (Instant Messages) oder E-Mail ebenso wie Telefongespräche. Neben leitungsvermittelnden Netzwerken, wie beispielsweise dem klassischen Telefonnetz, werden zunehmend paketvermittelnde Netze zum Aufbau von Kommunikationssystemen eingesetzt. Ein Beispiel ist hier das Internet, über das nicht nur unidirektional Textmeldungen übertragen werden können, sondern über das mit Voice over IP (VoIP) auch bidirektionale Sprachübertragung möglich ist.

Bei den paketvermittelnden Netzwerken lassen sich Netzwerke mit zentraler Architektur, auch Client Server Architektur genannt, und dezentraler Struktur unterscheiden. Netzwerke mit dezentraler Struktur, zum Beispiel die so genannten Peer to Peer-Netzwerke, weisen keine zentrale, das Netzwerk kontrollierende Einheit auf. Dezentrale Netzwerke zeichnen sich durch eine große Flexibilität aus, insbesondere was die Auf-

nahme neuer Teilnehmergeräte in das Netzwerk beziehungsweise das Ausgliedern von Teilnehmergeräten betrifft. Im Rahmen der Anmeldung werden Kommunikationssysteme mit dezentraler Netzwerkstruktur kurz als dezentrale Kommunikationssysteme bezeichnet.

In Kommunikationssystemen ist es wünschenswert, die Teilnehmer vor ungewollten Nachrichten zu schützen. Dazu ist bekannt, dass die Teilnehmer eines Kommunikationssystems andere Teilnehmer, von denen sie keine Nachrichten empfangen möchten, benennen. Üblicherweise wird zu diesem Zweck eine Senderausschlussliste, auch Black List genannt, erstellt, in der Adressinformationen aller Teilnehmer, von denen eine Nachricht nicht gewünscht ist, aufgeführt sind. Diese teilnehmerspezifische Senderauschlussliste kann beispielsweise in dem Teilnehmergerät des entsprechenden Teilnehmers hinterlegt sein. Bei dem Teilnehmergerät eingehende Nachrichten können anhand der Absenderinformationen entsprechend der hinterlegten Senderausschlussliste im Teilnehmergerät entsprechend gefiltert werden, und Nachrichten von ausgeschlossenen Teilnehmern unterdrückt werden.

Nachteilig bei einer Filterung eingehender Nachrichten im Teilnehmergerät ist, dass auch ungewünschte Nachricht zunächst bis zum Teilnehmergerät übermittelt werden müssen. Auf diese Weise belegen auch ungewünschte und letztlich unterdrückte Nachrichten unnötigerweise Netzwerkübertragungsbandbreite. Bei Kommunikationssystemen mit einer zentralen Netzwerkstruktur ist daher bekannt, die teilnehmerspezifischen Senderauschlusslisten in der oder einer der zentralen Einheiten, die für die Vermittlung und Weiterleitung von Nachrichten vorgesehen sind, abzulegen und zu vermittelnde Nachrichten bereits an dieser Stelle entsprechend der teilnehmerspezifischen Senderauschlusslisten zu beurteilen. Ungewünschte

Nachrichten brauchen dann gar nicht erst zum Teilnehmergerät weitergeleitet werden. Da die zentralen Vermittlungseinheiten eines solchen Kommunikationssystems üblicherweise als vertrauenswürdig angesehen werden können, ist das Vorhalten der einzelnen teilnehmerspezifischen Senderauschlusslisten unter datenschutztechnischem Aspekt als sicher einzustufen. Bei Kommunikationssystemen mit dezentraler Netzwerkstruktur ist eine solche Vorgehensweise aufgrund der fehlenden zentralen Vermittlungsstelle jedoch nicht möglich.

Es ist daher eine Aufgabe der vorliegenden Erfindung, Verfahren bereitzustellen, durch die auch in einem dezentralen Kommunikationssystem ein Weiterleiten von ungewünschten Nachrichten blockiert wird, wobei Datenschutzaspekte berücksichtigt werden.

Die Aufgabe wird gelöst durch die Merkmale der unabhängigen Patentansprüche. Vorteilhafte Ausgestaltungen der Erfindung sind in den jeweiligen abhängigen Ansprüchen gekennzeichnet.

Gemäß einem ersten Aspekt zeichnet sich die Erfindung durch ein Verfahren zum Erstellen einer teilnehmerspezifischen Senderauschlussliste für ein dezentrales Kommunikationssystem aus, das die folgenden Schritte aufweist: Es wird mindestens ein auszuschließender Sender durch Vorgabe von mindestens einer dem Sender zugeordneten Adressinformation angegeben. Anschließend wird zu jeder der vorgegebenen Adressinformationen eine unumkehrbar eindeutige Repräsentation erstellt. Alle unumkehrbar eindeutigen Repräsentationen werden in einer ersten Liste abgelegt, die daraufhin als teilnehmerspezifische Senderauschlussliste in dem dezentralen Kommunikationssystem abgelegt wird.

Dadurch, dass Adressinformationen nur in ihrer unumkehrbar eindeutigen Repräsentation enthalten sind, aus der eine Rekonstruktion der Adressinformationen im Klartext nicht möglich ist, ist auf einfache Weise möglich, die gestellten Anforderungen bezüglich des Datenschutzes zu erfüllen. Die teilnehmerspezifische Senderauschlussliste enthält dennoch genügend Informationen, um ungewünschte Sender zu identifizieren und Nachrichten solcher Sender bereits im Vorfeld, zum Beispiel beim Weiterleiten einer Nachricht, auszusondern.

Gemäß einer vorteilhaften Weiterbildung des ersten Aspekts wird zum Erstellen der unumkehrbar eindeutigen Repräsentationen der Adressinformationen ein Hashing-Verfahren, insbesondere SHA-1 (Secure Hash Algorithm) oder MD5 (Messenger Digest), eingesetzt. Dies ist kryptografisch sicher und unaufwändig zu implementieren.

In einer weiteren vorteilhaften Ausgestaltung des ersten Aspekts werden die folgenden zusätzlichen Schritte ausgeführt, bevor die teilnehmerspezifische Senderauschlussliste in dem dezentralen Kommunikationssystem abgelegt wird: Alle vorgegebenen Adressinformationen werden in einer zweiten Liste abgelegt, die daraufhin verschlüsselt wird. Danach wird die verschlüsselte zweite Liste zur teilnehmerspezifischen Senderauschlussliste hinzugefügt. Ein Teilnehmer, der über einen entsprechenden Schlüssel zum Entschlüsseln der zweiten Liste verfügt, wird auf diese Weise in die Lage versetzt, die Adressinformationen der auszuschließenden Sender aus der Senderauschlussliste wieder als Klartext zu extrahieren. Diesem Teilnehmer wird so ermöglicht, die Senderauschlussliste zu ergänzen oder abzuändern.

Hierbei ist besonders vorteilhaft, die zweite Liste entweder durch ein symmetrisches Verschlüsselungsverfahren zu ver-

schlüsseln oder durch ein asymmetrisches Verschlüsselungsverfahren, wobei als Schlüssel ein öffentlicher Schlüssel des Teilnehmers eingesetzt wird, für den die Senderauschlussliste spezifisch ist. Weiterhin kann vorteilhafterweise ein hybrides Verschlüsselungsverfahren eingesetzt werden.

In einer weiteren vorteilhaften Ausgestaltung des Verfahrens wird die teilnehmerspezifische Senderausschlussliste mit einer digitalen Unterschrift des Teilnehmers, für den die Senderausschlussliste spezifisch ist, versehen, bevor sie in dem dezentralen Kommunikationssystem abgelegt wird. Auf diese Weise kann die Authentizität der teilnehmerspezifischen Senderausschlussliste überprüft werden, was einem Missbrauch durch gefälschte Senderauschlusslisten vorbeugt. Besonders vorteilhaft wird dabei die digitale Unterschrift abhängig von einem privaten Schlüssel des Teilnehmers erstellt, für den die Senderauschlussliste spezifisch ist.

In einer weiteren vorteilhaften Ausgestaltung des Verfahrens werden die folgenden zusätzlichen Schritte ausgeführt: Es wird mindestens ein Bereich von Adressinformationen vorgegeben, wobei der Bereich Adressen umfasst, die auszuschließenden Sendern zugeordnet sind. Der mindestens eine vorgegebene Bereich wird in der ersten Liste abgelegt. Besonders vorteilhaft ist der Bereich von Adressinformationen durch eine Adressinformation, die Platzhalter umfasst, festgelegt. Adressbereiche werden somit in der Senderauschlussliste im Klartext geführt, um eine Auswertung von Platzhaltern zu ermöglichen. Da bei derart angegebenen Adressbereiche einzelne von dem Bereich umfasste konkreten Adressen unbestimmt sind, ist dieses Verfahren datenschutztechnisch nicht kritisch.

Gemäß einem zweiten Aspekt wird die Aufgabe durch ein Verfahren zum Weiterleiten einer Nachricht in einem dezentralen

Kommunikationssystem gelöst. Das Verfahren gemäß des zweiten Aspekts umfasst die folgenden Schritte: Es wird eine Nachricht eines Senders mit einer dem Sender zugeordneten Adressinformation zur Weiterleitung an einen Adressat in dem dezentralen Kommunikationssystem entgegengenommen. Daraufhin wird eine für den Adressat spezifische Senderauschlussliste aus dem dezentralen Kommunikationssystem eingelesen. Zu der Adressinformation des Senders wird eine unumkehrbar eindeutige Repräsentation erstellt und diese mit den Einträgen der eingelesenen teilnehmerspezifischen Senderauschlussliste verglichen. Falls die unumkehrbar eindeutige Repräsentation der Adressinformation des Senders keinem der Einträge der teilnehmerspezifischen Senderauschlussliste entspricht, wird die Nachricht an den Adressat weitergeleitet.

Dieses Verfahren gibt an, wie eine gemäß dem ersten Aspekt der Erfindung erstellte teilnehmerspezifische Senderauschlussliste beim Weiterleiten einer Nachricht ausgewertet wird. Die sich ergebenden Vorteile dieses zweiten Aspekts der Erfindung entsprechen denen des ersten Aspekts.

Gemäß einer vorteilhaften Weiterbildung des zweiten Aspekts werden die folgenden zusätzlichen Schritte durchgeführt: Es wird überprüft, ob die teilnehmerspezifische Senderauschlussliste mit einer digitalen Unterschrift versehen ist. Falls sie mit einer digitalen Unterschrift versehen ist, wird anhand der digitalen Unterschrift die Authentizität der Senderauschlussliste überprüft. Wenn die digitale Unterschrift den Adressat nicht ausweist, wird die Nachricht in jedem Fall weitergeleitet.

Gemäß einem dritten Aspekt wird die Aufgabe gelöst durch ein Computerprogrammprodukt mit Programmcode zur Ausführung auf einem Teilnehmergerät, das zum Betrieb in einem dezentralen

Kommunikationssystem geeignet ist. Das Computerprogrammprodukt zeichnet sich dadurch aus, dass bei der Ausführung des Programmcodes eines der angegebenen Verfahren ausgeführt wird. Die sich ergebenden Vorteile entsprechen denen des ersten und zweiten Aspekts.

Die Erfindung wird nachfolgend anhand von Ausführungsbeispielen mit Hilfe von vier Figuren näher erläutert. Die Figuren zeigen:

Figur 1 eine Kommunikationssystem mit vier Teilnehmergeräten in einer schematischen Darstellung,

Figur 2 ein Flussdiagramm eines Verfahrens zum Erstellen einer teilnehmerspezifischen Senderauschlussliste,

Figur 3 eine schematische Darstellung einer teilnehmerspezifischen Senderauschlussliste und

Figur 4 ein Flussdiagramm eines Verfahrens zum Weiterleiten einer Nachricht in einem dezentralen Kommunikationssystem.

In Figur 1 ist schematisch ein dezentrales Kommunikationssystem dargestellt. Das dezentrale Kommunikationssystem umfasst vier Teilnehmergeräte: einen Sender 1, einen Adressat 2 und zwei weitere Teilnehmer 3 und 4. Eine vom Adressat 2 erstellte teilnehmerspezifische Senderausschlussliste L ist bei dem weiteren Teilnehmer 4 abgelegt. Von dem Sender 1 wird eine Nachricht 5 mit Adressinformationen A_S des Senders 1 und Adressinformation A_A des Adressaten 2 an den weiteren Teilnehmer 3 zur Weiterleitung zum Adressat 2 geschickt. Die Begriffe Teilnehmer und Teilnehmergerät werden im Rahmen der Anmeldung teilweise synonym gebraucht, wenn die Unterscheidung für

den betrachteten Zusammenhang unerheblich ist bzw. sich aus dem Zusammenhang ergibt.

Das in Figur 1 gezeigte schematische dezentrale Kommunikationssystem basiert beispielsweise auf einem Netzwerk mit Peer-to-Peer-Architektur. In der Figur ist dieses durch gestrichelte Linien angedeutet, durch die jeder der Teilnehmer mit jedem weiteren Teilnehmer des Kommunikationssystems verbunden ist. Die einzelnen Verbindungen sind dabei insofern als logische Verbindungen zu verstehen, als dass ein Netzwerk in Peer-to-Peer-Struktur auch auf Grundlage eines physikalisch andersartig strukturierten Netzwerkes aufgebaut werden kann. Peer-to-Peer-Netzwerke können beispielsweise als Subnetze im Internet realisiert werden. Wichtig ist, dass die Möglichkeit besteht, von jedem der Teilnehmer zu jedem weiteren Teilnehmer Informationen ohne Zwischenschaltung einer dedizierten zentralen Instanz des Netzwerks zu versenden und dass die Möglichkeit besteht, Suchanfragen an alle Teilnehmer des Netzes zu schicken, beispielsweise in Form so genannter Multicast-Anfragen oder unter Verwendung von Verfahren basierend auf verteilten (Hash-) Tabellen.

In Figur 1 sind solche Suchanfragen als kurze, von einem Teilnehmer in jede Richtung ausgehende Pfeile dargestellt. Lange, zwei Teilnehmer verbindende Pfeile kennzeichnen den Austausch von Daten. Die ausgetauschten Daten sind jeweils entlang der Pfeile symbolisiert.

Figur 1 skizziert das dezentrales Kommunikationssystem in einer Situation, in der die teilnehmerspezifische Senderausschlussliste L des Adressaten 2 bei der Weiterleitung einer von dem Sender 1 an den Adressat 2 adressierten Nachricht durch den weiteren Teilnehmer 3 ausgewertet wird. Das Vorgehen diesbezüglich ist im Folgenden zur Übersicht zunächst

grob skizziert. Detaillierte Ausführungsbeispiele sind danach im Zusammenhang mit den Figuren 2 und 4 beschrieben. Eine mögliche Ausgestaltung der teilnehmerspezifischen Senderausschlussliste L wird im Zusammenhang mit Figur 3 angegeben.

Der Adressat 2 erstellt eine für ihn spezifische Senderausschlussliste L und legt diese dezentral im Kommunikationssystem ab. Vorgehensweisen, mittels derer Daten dezentral in einem Peer-to-Peer-Netzwerk gespeichert werden können, sind dabei aus dem Stand der Technik bekannt. Beispielsweise kann zu diesem Zweck eine Suchanfrage bezüglich des Speicherns an die weiteren Teilnehmer des Netzwerks gesendet werden. Die Teilnehmer handeln daraufhin untereinander aus, welcher oder welche der Teilnehmer zum Abspeichern der Daten geeignet und bereit sind. An den oder diese Teilnehmer verschickt der die Speicheranfrage stellende Teilnehmer daraufhin die Daten. Häufig werden Daten dabei aus Sicherheitsgründen redundant bei mehreren Teilnehmern vorgehalten. In dem in Figur 1 dargestellten Beispiel hat der weitere Teilnehmer 4 auf die Speicheranfrage des Teilnehmers 2 bezüglich einer dezentralen Speicherung der für ihn spezifischen Senderausschlussliste L geantwortet, so dass ihm die Senderausschlussliste L zur Speicherung übertragen wird.

Das dezentrale Kommunikationssystem ist grundsätzlich so ausgelegt, dass Nachrichten von jedem Teilnehmer zu jedem Teilnehmer gesendet werden können, der genaue Weg, den die Daten dabei gehen, ist jedoch nicht vorbestimmt. Weiterhin kann das dezentrale Kommunikationssysteme in mehrere Subnetze zerfallen, innerhalb derer die jeweiligen Teilnehmer direkt miteinander kommunizieren können, die einzelnen Subnetze aber nur über einen oder mehrere Teilnehmer verbunden sind. In einem solchen Fall fungieren die Teilnehmer aus der Schnittmenge

zweier oder mehrerer Subnetze als Relaisstationen zur Vermittlung und Weiterleitung von Nachrichten.

In Figur 1 wird beispielsweise eine vom Sender 1 an den Adressat 2 gerichtete Nachricht 5 über den weiteren Teilnehmer 3 geleitet. Vor einer Weiterleitung der Nachricht an den Adressat 2 erfragt der weitere Teilnehmer 3 die teilnehmerspezifische Senderausschlussliste L des Adressaten 2 aus dem dezentralen Kommunikationsnetz. Diese geschieht wiederum durch eine Suchanfrage. Der weitere Teilnehmer 3 erhält die angefragte teilnehmerspezifische Senderausschlussliste L daraufhin von dem weiteren Teilnehmer 4 übermittelt. Anhand der teilnehmerspezifischen Sendeausschlussliste L überprüft der weitere Teilnehmer 3 daraufhin, ob Nachrichten des Senders 1 von dem Adressaten 2 erwünscht sind oder nicht und leitet entsprechend die Nachricht weiter oder unterdrückt sie.

In Figur 2 ist ein Ausführungsbeispiel eines Verfahrens zum Erstellen einer teilnehmerspezifischen Senderausschlussliste in einem Flussdiagramm detaillierter dargestellt. Beispielhaft ist das Verfahren für die in Figur 1 gezeigte Situation angegeben, also mit dem Sender 1, dem Adressaten 2 und den weiteren Teilnehmern 3 und 4.

In einem Schritt S1 wird ein Sender, von dem ein Teilnehmer keine Nachrichten erhalten möchte, vorgegeben. Dieses kann beispielsweise dadurch geschehen, dass der Teilnehmer mindestens eine dem auszuschließenden Sender zugeordnete Adressinformation A_n vorgibt. Adressen können dabei, je nach Kommunikationssystem in unterschiedlichsten Formaten angegeben sein, z.B. in Form von Nummern, Namen, oder als E-Mail Adressen oder als SIP-URI (Session Initiation Protocol - Uniform Ressource Identifier). Jedes Format, das auch zur Adressangabe beim Versenden einer Nachricht eingesetzt werden kann, ist

auch in diesem Verfahrensschritt zur Vorgabe des auszuschließenden Absenders geeignet.

In einem Schritt S2 wird eine unumkehrbar eindeutige Repräsentation der vorgegebenen Adressinformation A_n erstellt. Eine solche Repräsentation ist charakteristisch und eindeutig für die vorgegebene Adressinformation A_n, erlaubt jedoch nicht das Rekonstruieren der Adressinformation A_n. Beispiele bekannter Transformationen mit dieser Eigenschaft, auch Hashing-Verfahren genannt, sind SHA-1 oder MD5. Die erstellte eindeutige Repräsentation wird daraufhin einer ersten Liste L_1 zugefügt. In einem Schritt S3 wird die Adressinformation A_n darüber hinaus im Klartext, also ohne vorherige Transformation, einer zweiten Liste L_2 zugefügt.

In einem Schritt S4 wird abgefragt, ob weitere Sender auszuschließen sind oder ob ein bereits ausgeschlossener Sender noch zusätzlich mit seiner Kennung in einem anderen Format aufgenommen werden soll. Gegebenenfalls werden dann die Schritte S1 bis S3 wiederholt. Nachdem auf diese Weise die erste und zweite Liste mit den eindeutigen Repräsentationen beziehungsweise dem Klartext der vorgegebenen Adressinformationen A_n erstellt sind, wird das Verfahren in einem Schritt S5 fortgesetzt.

In dem Schritt S5 wird die zweite Liste L_2, die die Adressinformationen im Klartext enthält, als Ganzes zur verschlüsselten zweiten Liste L_2^* verschlüsselt. Dabei kann beispielsweise ein symmetrisches Verschlüsselungsverfahren oder auch ein asymmetrisches Verschlüsselungsverfahren mit einem Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel, eingesetzt werden. Alternativ ist möglich ein so genanntes hybrides Verschlüsselungsverfahren einzusetzen, bei dem ein symmetrischer, zur tatsächlichen Verschlüsselung der

Information eingesetzter Schlüssel seinerseits durch ein asymmetrisches Verschlüsselungsverfahren geschützt wird. Der Schlüssel sollte dabei nur dem Teilnehmer, der die auszuschließenden Teilnehmerinformationen vorgibt und für den zu erstellende Senderausschlussliste spezifisch ist, bekannt sein. Wird ein asymmetrisches oder hybrides Verschlüsselungsverfahren eingesetzt, sollte der öffentliche Schüssel des Schlüsselpaares genutzt werden.

In einem Schritt S6 werden die erste Liste L_1 und die verschlüsselte zweite Liste L_2^* zu der teilnehmerspezifischen Sendeausschlussliste L zusammengeführt.

In einem Schritt S7 wird die erstellte Sendeausschlussliste L mit einer digitalen Unterschrift versehen. Durch die digitale Unterschrift kann später die Authentizität der Sendeausschlussliste überprüft werden. Es kann eine beliebige, aus dem Stand der Technik bekannte Methode zum Erstellen digitaler Unterschriften eingesetzt werden. Es ist möglich, eine digitale Unterschrift mit Hilfe des privaten Schlüssels des bereits beim Verschlüsseln der zweiten Liste eingesetzten Schüsselpaares des Teilnehmers vorzunehmen, vorzugsweise werden aber für Verschlüsselung und digitale Signatur zwei unterschiedliche Schlüsselpaare verwendet.

Die auf diese Weise erstellte und unterschriebene teilnehmerspezifische Senderausschlussliste wird in einem Schritt S8 daraufhin dezentral im Kommunikationssystem abgelegt. Wie bereits erwähnt, sind hierzu geeignete Vorgehensweisen in Netzwerken mit dezentraler Architektur bekannt.

Eine gemäß diesem Verfahren erstellte teilnehmerspezifische Senderausschlussliste L ist in Figur 3 schematisch dargestellt. Sie umfasst die erste Liste L_1 mit Einträgen L_1a bis

L_1d, die die unumkehrbar eindeutigen Repräsentationen der jeweils vorgegebenen Adressinformationen A_n aufweisen. In der zweiten Liste L_2 sind diese vorgegebenen Adressinformationen A_n als Einträge L_2a bis L_2d im Klartext enthalten. Die teilnehmerspezifische Senderausschlussliste L umfasst diese zweite Liste L_2 als verschlüsselte zweite Liste L_2^* und ist mit einer digitalen Unterschrift 6 versehen.

Die erste Liste L_1 kann von jedem Teilnehmer des Kommunikationssystems genutzt werden, um zu überprüfen, ob ein Sender einer Nachricht in der teilnehmerspezifischen Senderausschlussliste L gelistet ist. Die Einträge L_2 a-d der zweiten Liste L_2 können hingegen genutzt werden, um die Senderauschlussliste L zu ergänzen oder abzuändern. Dieses setzt jedoch einen entsprechenden Schlüssel zum Entschlüsseln der verschlüsselten zweiten Liste L_2^* voraus, da die zweite Liste L_2 nur in ihrer verschlüsselten Fassung in der Senderauschlussliste L enthalten ist. Üblicherweise wird nur der Teilnehmer, hier der Adressat 2, der die Senderauschlussliste L erstellt hat und für den sie spezifisch ist, über diesen Schlüssel verfügen. Der Teilnehmer braucht die zweite Liste L_2 mit den Einträgen L_2 a-d im Klartext nicht lokal auf seinem Teilnehmergerät vorhalten, sondern kann sie jederzeit wieder aus der Senderauschlussliste L extrahieren. Das ermöglicht dem Teilnehmer auch, die Senderauschlussliste L von verschiedenen Geräten aus zu ergänzen oder abzuändern. Ein Synchronisationsproblem durch lokal auf verschiedenen Teilnehmergeräten vorgehaltenen zweiten Listen wird so umgangen, ohne Datenschutzaspekte zu vernachlässigen.

In Figur 4 ist als Flussdiagramm ein Ausführungsbeispiel eines Verfahrens zum Weiterleiten einer Nachricht in einem dezentralen Kommunikationssystem dargestellt, wie es beispiels-

weise in dem in Figur 1 gezeigten Ausführungsbeispiel von dem weiteren Teilnehmer 3 ausgeführt werden kann.

In einem ersten Schritt S11 des Verfahrens nimmt das weitere Teilnehmergerät 3 die Nachricht 5 des Senders 1 entgegen. In der Nachricht sind zusätzliche Informationen enthalten oder vorangestellt. Für das Verfahren ist hier insbesondere die Adressinformation A_S des Senders 1 und die Adressinformation A_A des Adressaten 2 von Bedeutung.

In einem Schritt S12 wird anhand der Adressinformationen A_A des Adressaten 2 dessen teilnehmerspezifische Senderausschlussliste L aus dem dezentralen Kommunikationssystem eingelesen. Anschließend wird in einem Schritt S13 eine unumkehrbar eindeutige Repräsentation der Adressinformationen A_S des Senders 1 erstellt.

In einem Schritt S14 wird diese unumkehrbar eindeutige Repräsentation mit den Einträgen der ersten Liste L_1 der teilnehmerspezifischen Senderausschlussliste L verglichen. Falls für keinen der Einträge L_1a bis L_1d der ersten Liste L_1 Gleichheit mit der unumkehrbar eindeutigen Repräsentation der Adressinformationen A_S des Senders 1 festgestellt wird, verzweigt das Verfahren zu einem Schritt S16 in dem die Nachricht 5 an den Adressat 2 weitergeleitet wird. Das Verfahren endet danach.

Wird dagegen in dem Schritt S14 eine Übereinstimmung in einem Eintrag gefunden, bedeutet das, dass Nachrichten des Senders 1 von dem Adressat 2 gemäß der teilnehmerspezifischen Senderausschlussliste L nicht erwünscht sind.

Bevor anhand dieser Feststellung Konsequenzen bezüglich der Weiterleitung der Nachricht gezogen werden, wird in einem Schritt S15 zunächst die Authentizität der teilnehmerspezifi-

schen Senderausschlussliste L anhand der digitalen Unterschrift 6 überprüft. Falls die digitale Unterschrift 6 mit Hilfe eines privaten Schlüssels erstellt wurde, wird hierzu der zugehörige öffentliche Schlüssel benötigt. Es kann vorgesehen sein, dass die einzelnen Teilnehmer des Kommunikationssystems über Listen mit den öffentlichen Schlüsseln der weiteren Teilnehmer verfügen, insbesondere wenn innerhalb des dezentralen Kommunikationssystems häufig Anwendung genutzt werden, die einen verschlüsselten Datenaustausch einsetzen. Alternativ kann vorgesehen sein, dass ein öffentlicher Schlüssel eines Teilnehmers im Bedarfsfall von dem entsprechenden Teilnehmergerät angefordert wird. Weiterhin ist möglich, die öffentlichen Schlüssel von Teilnehmern beispielsweise in Form digitaler Zertifikate dezentral im Kommunikationssystem zu speichern. Vorzugsweise werden solche digitalen Zertifikate dann den teilnehmerspezifischen Senderausschlussliste L beigefügt und sind damit zur Überprüfung der digitalen Unterschrift grundsätzlich verfügbar.

Wird in dem Schritt S15 festgestellt, dass die empfangene teilnehmerspezifische Senderausschlussliste L nicht eindeutig als von dem Adressat 2 erstellte, authentische Liste identifiziert werden kann, wird die in Schritt S14 getroffene Feststellung nicht weiter berücksichtigt und das Verfahren verzweigt ebenfalls zum Schritt S16 zur Weiterleitung der Nachricht 5.

Wird in Schritt S15 die Senderausschlussliste dagegen als authentisch eingestuft, wird daraufhin die Nachricht 6 vom weiteren Teilnehmergerät 3 verworfen und nicht weitergeleitet. An dieser Stelle kann zusätzlich eine Benachrichtigung des Senders 1 über die Ablehnung der Nachricht 5 erfolgen. Weiterhin ist denkbar, dass auch der Adressat 2 über den Eingang der ungewünschten Nachricht 5 informiert wird. Optional kann

die Nachricht auch vom weiteren Teilnehmergerät 3 gespeichert werden, um bei Bedarf noch nachträglich vom Adressat 2 abgerufen werden zu können.

Die Reihenfolge der Überprüfungen von Schritt S14 und S15 kann in weiteren Ausgestaltungen des Verfahrens auch insofern geändert werden, dass die Überprüfung der Authentizität der teilnehmerspezifische Senderausschlussliste L (Schritt S15) dem Vergleich der unumkehrbar eindeutigen Repräsentation der Adressinformationen A_S des Senders 1 mit den Einträgen der teilnehmerspezifische Senderausschlussliste L (Schritt S14) vorangestellt wird. Da eine Überprüfung digitaler Unterschriften im Allgemeinen rechenaufwändig ist, ist aus Performancegründen die dargestellte Reihenfolge bevorzugt. Eine Überprüfung der digitalen Unterschrift 6 ist im dargestellten Fall nicht zwingend, sondern erfolgt nur, wenn von Schritt S14 nicht zur Weiterleitung der Nachricht 5 nach Schritt S16 verzweigt wurde.

Patentansprüche

1. Verfahren zum Erstellen einer teilnehmerspezifischen Senderausschlussliste (L) für ein dezentrales Kommunikationssystem mit den Schritten:

- Angeben mindestens eines auszuschließenden Senders durch Vorgeben von mindestens einer dem Sender zugeordneten Adressinformation,
- Erstellen einer unumkehrbar eindeutigen Repräsentation zu jeder der vorgegebenen Adressinformationen,
- Ablegen aller unumkehrbar eindeutigen Repräsentation in einer ersten Liste (L_1),
- Ablegen der ersten Liste (L_1) als teilnehmerspezifische Senderausschlussliste (L) in dem dezentralen Kommunikationssystem.

2. Verfahren nach Anspruch 1, bei dem zum Erstellen der unumkehrbar eindeutigen Repräsentation (L_1 a-d) ein Hashing-Verfahren, insbesondere SHA-1 oder MD5, eingesetzt wird.

3. Verfahren nach einem der Ansprüche 1 oder 2, bei dem die folgenden zusätzlichen Schritten ausgeführt werden, bevor die teilnehmerspezifische Senderausschlussliste (L) in dem dezentralen Kommunikationssystem abgelegt wird:

- Ablegen aller der vorgegebenen Adressinformationen in einer zweiten Liste (L_2),
- Verschlüsseln der zweiten Liste (L_2) zur verschlüsselten zweiten Liste (L_2^*),
- Hinzufügen der verschlüsselten zweiten Liste (L_2^*) zur teilnehmerspezifische Senderausschlussliste (L).

4. Verfahren nach Anspruch 3, bei dem zum Verschlüsseln der zweiten Liste (L_2) ein symmetrisches Verschlüsselungsverfahren eingesetzt wird.

5. Verfahren nach Anspruch 3, bei dem zum Verschlüsseln der zweiten Liste (L_2) ein asymmetrisches Verschlüsselungsverfahren eingesetzt wird und als Schlüssel ein privater Schlüssel des Teilnehmers eingesetzt wird, für den die Senderausschlussliste (L) spezifisch ist.

6. Verfahren nach Anspruch 3, bei dem ein hybrides Verschlüsselungsverfahren eingesetzt wird.

7. Verfahren nach einem der Ansprüche 1 bis 6, bei dem die teilnehmerspezifische Senderausschlussliste (L) mit einer digitalen Unterschrift (6) des Teilnehmers, für den sie spezifisch ist, versehen wird, bevor sie in dem dezentralen Kommunikationssystem abgelegt wird.

8. Verfahren nach Anspruch 7, bei dem die digitale Unterschrift (6) abhängig von einem privaten Schlüssel des Teilnehmers erstellt wird.

9. Verfahren nach einem der Ansprüche 1 bis 8, mit den folgenden zusätzlichen Schritten

- Vorgeben von mindestens einem Bereich von Adressinformationen, wobei der Bereich Adressen umfasst, die auszuschließenden Sendern zugeordnet sind,
- Ablegen des vorgegebenen Bereichs in der ersten Liste (L_1).

10. Verfahren nach Anspruch 9, bei dem der Bereich von Adressinformationen durch eine Adresseinformation, die Platzhalter umfasst, festgelegt ist.

11. Verfahren zum Weiterleiten einer Nachricht (5) in einem dezentralen Kommunikationssystem mit den Schritten:

- Entgegennehmen einer Nachricht (5) eines Senders (1) mit einer dem Sender (1) zugeordneten Adressinformation (A_S) zur Weiterleitung an einen Adressat (2) in dem dezentralen Kommunikationssystem,
- Einlesen einer für den Adressat (2) spezifischen Senderausschlussliste (L) aus dem dezentralen Kommunikationssystem,
- Erstellen einer unumkehrbar eindeutigen Repräsentationen der Adressinformation (A_S) des Senders (1),
- Vergleich der unumkehrbar eindeutigen Repräsentationen der Adressinformation (A_S) des Senders (1) mit Einträgen der teilnehmerspezifischen Senderausschlussliste (L) und,
- falls die unumkehrbar eindeutigen Repräsentation der Adressinformation (A_S) des Senders (1) keinem der Einträge (L_1) der teilnehmerspezifischen Senderausschlussliste (L) entspricht, Weiterleiten der Nachricht (5) an den Adressat (2).

12. Verfahren nach Anspruch 11, mit den zusätzlichen folgenden Schritten, falls die teilnehmerspezifische Senderausschlussliste (L) Einträge (L_1) aufweist, mit denen Bereiche von Adressinformationen festgelegt sind:

- Vergleichen der Adressinformation (A_S) des Senders (1) mit den Einträgen (L_1), durch die Bereiche von Adressinformationen festgelegt sind und,
- Weiterleiten der Nachricht (5) an den Adressat (2) nur, wenn die unumkehrbar eindeutigen Repräsentation der Adressinformation (A_S) des Senders (1) keinem der Einträge (L_1) der teilnehmerspezifischen Senderausschlussliste (L) entspricht und wenn die Adressinformation (A_S) aus keinem der durch die Einträge (L_1) der teilnehmerspezifischen Senderausschlussliste (L) festgelegten Bereiche stammt.

13. Verfahren nach einem der Ansprüche 11 oder 12, mit den folgenden zusätzlichen Schritten:

- Überprüfen, ob die teilnehmerspezifischen Senderausschlussliste (L) mit einer digitalen Unterschrift (6) versehen ist und, falls sie mit einer digitalen Unterschrift (6) versehen ist,
- Überprüfen der digitalen Unterschrift (6),

wobei die Nachricht (5) in jedem Fall weitergeleitet wird, wenn die digitales Unterschrift (6) den Adressat (2) nicht ausweist.

14. Verfahren nach Anspruch 13, bei dem die digitale Unterschrift (6) mit einem öffentlichen Schlüssel des Adressaten (2) überprüft wird.

15. Computerprogrammprodukt mit Programmcode zur Ausführung eines Programms auf einem Teilnehmergerät, das zum Betrieb in einem dezentralen Kommunikationssystem geeignet ist, dadurch gekennzeichnet, dass bei der Ausführung des Programmcodes ein Verfahren nach einem der Ansprüche 1 bis 13 ausgeführt wird.

FIG 1

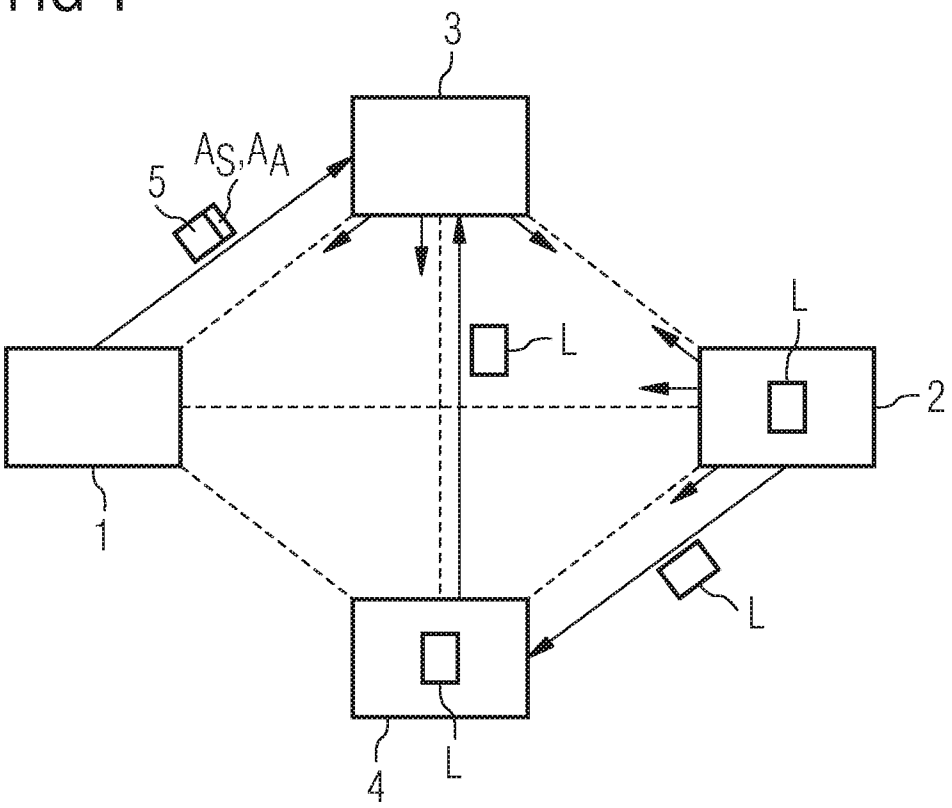


FIG 2

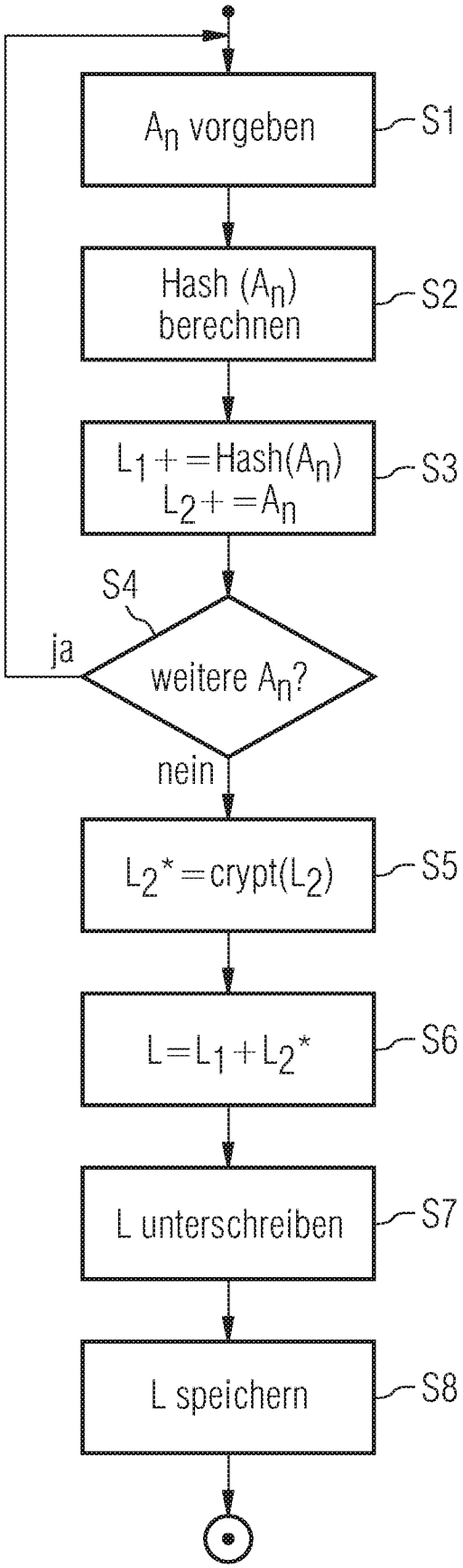

A_n vorgeben
S1
Hash (A_n) berechnen
S2
$L_1 += Hash(A_n)$
$L_2 += A_n$
S3
S4
ja
weitere A_n?
nein
$L_2^* = crypt(L_2)$
S5
$L = L_1 + L_2^*$
S6
L unterschreiben
S7
L speichern
S8

FIG 3

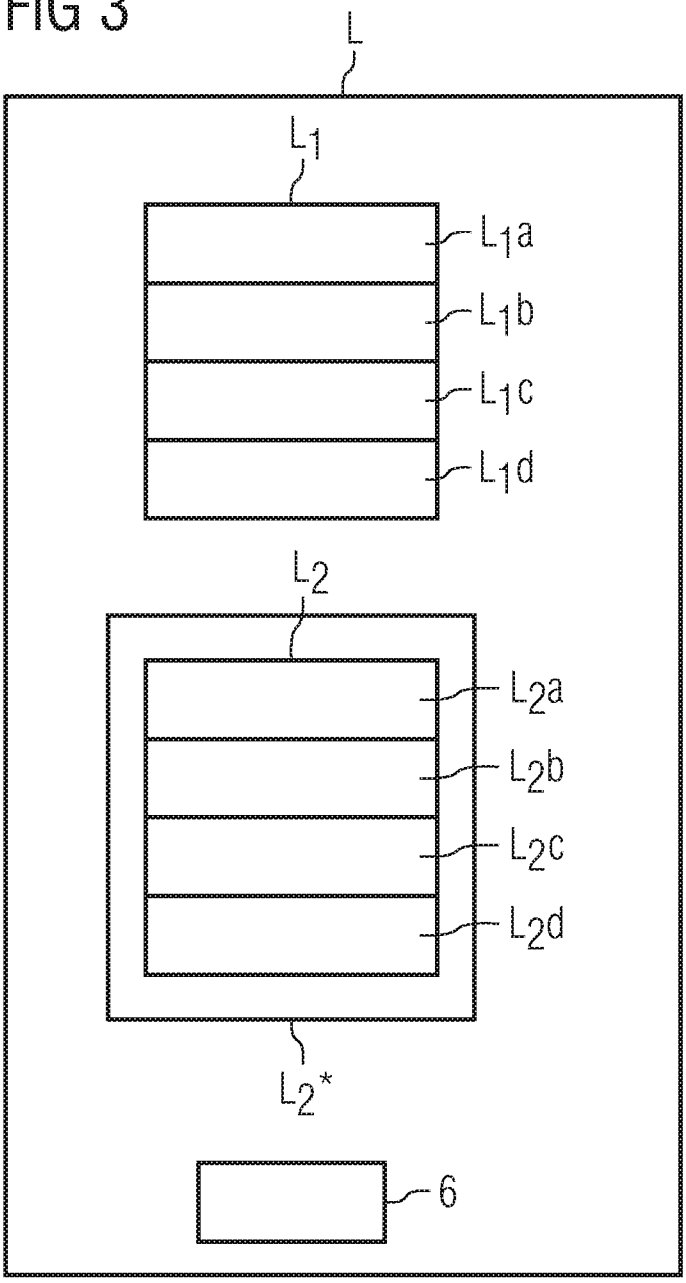
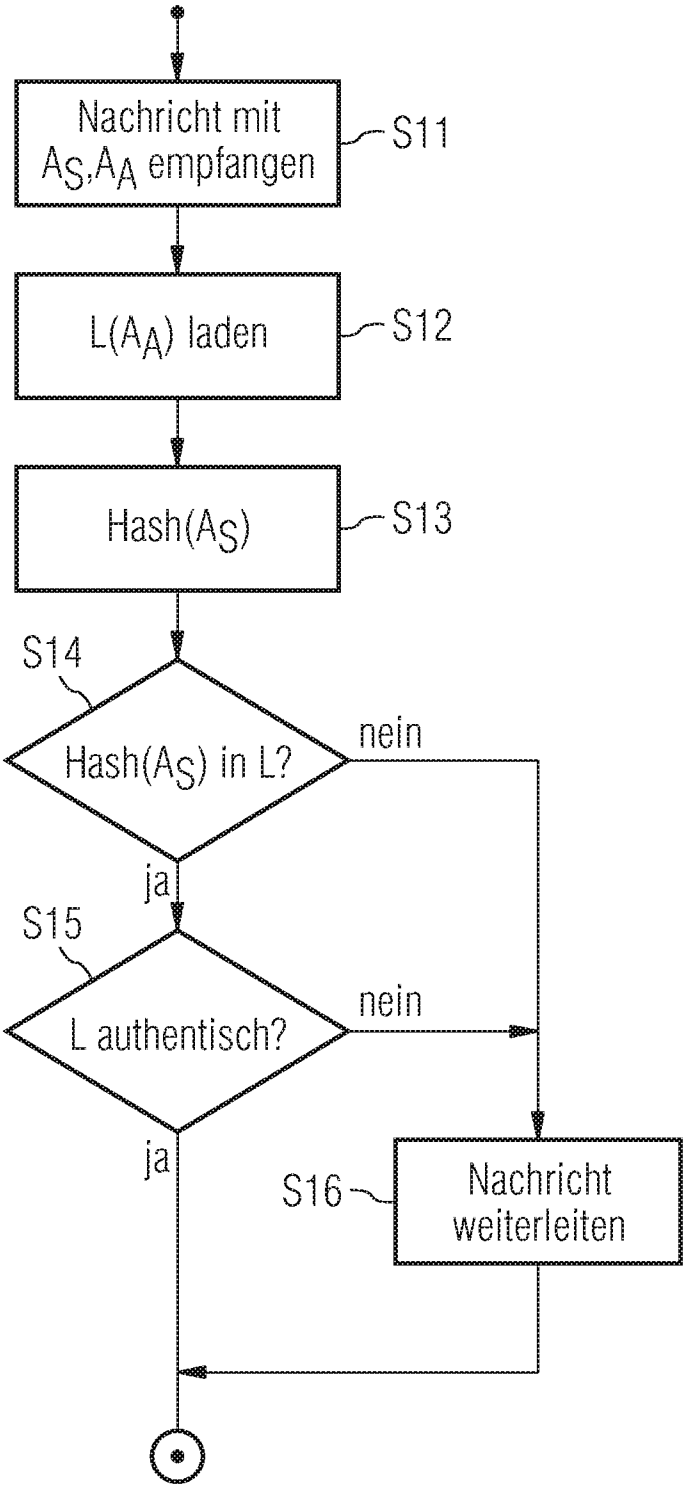


FIG 4


Nachricht mit A_S,A_A empfangen
S11
$L(A_A)$ laden
S12
Hash(A_S)
S13
S14
Hash(A_S) in L?
nein
ja
S15
L authentisch?
nein
ja
S16
Nachricht weiterleiten