(19) Deutsches Patent- und Markenamt

(10) **DE 10 2012 215 326 A1** 2014.03.06

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2012 215 326.8**
(22) Anmeldetag: **29.08.2012**
(43) Offenlegungstag: **06.03.2014**

(51) Int Cl.: ***H04L 9/28*** (2006.01)

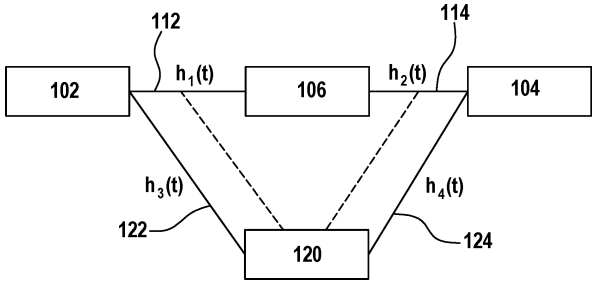
(71) Anmelder:
Robert Bosch GmbH, 70469, Stuttgart, DE

(72) Erfinder:
Mueller, Andreas, 71336, Waiblingen, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren und Vorrichtung zur Ermittlung eines kryptografischen Schlüssels in einem Netzwerk**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Erzeugung eines kryptografischen Schlüssels in einem Netzwerk mit einem ersten Netzwerkelement (102), einem zweiten Netzwerkelement (104) und einem Netzwerkknoten (106), wobei das erste Netzwerkelement über einen ersten Übertragungskanal (112) und das zweite Netzwerkelement über einen zweiten Übertragungskanal (114) mit dem Netzwerkknoten kommunizieren kann. Das Verfahren umfasst aufseiten des ersten Netzwerkelements einen Schritt des Bestimmens einer ersten Kanalinformation bezüglich des ersten Übertragungskanals basierend auf einem von dem Netzwerkknoten ausgesendeten ersten Pilotsignal und einen Schritt des Ermittelns des symmetrischen kryptografischen Schlüssels unter Verwendung der ersten Kanalinformation und einer Information über eine kombinierte Kanalinformation, wobei die kombinierte Kanalinformation eine seitens des Netzwerkknotens basierend auf einem von dem ersten Netzwerkelement zu dem Netzwerknoten übertragenen zweiten Pilotsignal und einem von dem zweiten Netzwerkelement zu dem Netzwerknoten übertragenen dritten Pilotsignal bestimmte Kombination von Übertragungscharakteristiken des ersten und des zweiten Übertragungskanals (112, 114) repräsentiert.



Beschreibung

Stand der Technik

[0001] Die vorliegende Erfindung bezieht sich auf ein Verfahren zur Ermittlung eines kryptografischen Schlüssels in einem Netzwerk, auf ein Verfahren zur Unterstützung einer Ermittlung von symmetrischen kryptografischen Schlüsseln in einem Netzwerk, auf eine entsprechende Vorrichtung sowie auf ein entsprechendes Computerprogrammprodukt.

[0002] Die Wahrung der Vertraulichkeit von zu übertragenden Daten stellt eines der wesentlichen Schutzziele im Bereich der Kommunikationssicherheit dar. Hierzu werden üblicherweise geeignete Verschlüsselungsverfahren eingesetzt, d. h. die jeweiligen Daten werden nicht im Klartext übertragen, sondern zunächst senderseitig verschlüsselt, um dann empfängerseitig wieder entschlüsselt zu werden. Ein potenzieller Angreifer, der nur die gesendeten Signale mithören kann, ist daher nicht ohne Weiteres in der Lage, die ursprünglichen Daten im Klartext zu rekonstruieren.

[0003] Eine solche Verschlüsselung von vertraulichen Daten ist insbesondere bei drahtlosen Kommunikationssystemen von Bedeutung, da hierbei ein abgestrahltes Signal ohne großen Aufwand immer auch von einem sich in der Nähe befindlichen potenziellen Angreifer empfangen und mitgehört werden kann. Nichtsdestotrotz spielt dies aber natürlich auch bei drahtgebundenen Systemen oftmals eine sehr wichtige Rolle.

[0004] Herkömmlicherweise gibt es zwei verschiedene Ansätze für entsprechende Verschlüsselungsverfahren. Bei symmetrischen Verfahren besitzen Sender (Alice) und Empfänger (Bob) denselben Schlüssel. Bei asymmetrischen Verfahren verschlüsselt der Sender die zu übertragenden Daten mit dem öffentlichen (d. h. auch einem potenziellen Angreifer möglicherweise bekannten) Schlüssel des Empfängers. Die Entschlüsselung kann aber nur mit dem zugehörigen privaten Schlüssel erfolgen, der idealerweise nur dem Empfänger bekannt ist.

Offenbarung der Erfindung

[0005] Vor diesem Hintergrund wird mit der vorliegenden Erfindung ein Verfahren zur Ermittlung eines kryptografischen Schlüssels in einem Netzwerk, ein Verfahren zur Unterstützung einer Ermittlung von symmetrischen kryptografischen Schlüsseln in einem Netzwerk, weiterhin eine Vorrichtung, die dieses Verfahren verwendet sowie schließlich ein entsprechendes Computerprogrammprodukt gemäß den Hauptansprüchen vorgestellt. Vorteilhafte Ausgestaltungen ergeben sich aus den jeweiligen Unteransprüchen und der nachfolgenden Beschreibung.

[0006] Gemäß dem vorliegend beschriebenen Ansatz können zwei Netzwerkelemente (Alice und Bob), die in einem Netzwerk über einen Netzwerkknoten miteinander kommunizieren können, jeweils denselben Schlüssel erzeugen. Die von den beiden Netzwerkelementen erzeugten Schlüssel können bei einer anschließenden Datenübertragung zwischen den beiden Netzwerkelementen für ein symmetrisches Verschlüsselungsverfahren genutzt werden. Zur Erzeugung der Schlüssel können die Netzwerkelemente auf Daten zurückgreifen, die sie von dem Netzwerkknoten erhalten können. Insbesondere können zur Erzeugung der Schlüssel Informationen über zumindest einen Übertragungskanal zwischen den Netzwerkelementen verwendet werden. Solche Informationen können sich beispielsweise auf eine Übertragungscharakteristik des Übertragungskanals beziehen.

[0007] Ein solches Verfahren zur Ermittlung eines kryptografischen Schlüssels in einem Netzwerk mit einem ersten Netzwerkelement, einem zweiten Netzwerkelement und einem Netzwerkknoten, wobei das erste Netzwerkelement über einen ersten Übertragungskanal und das zweite Netzwerkelement über einen zweiten Übertragungskanal mit dem Netzwerkknoten kommunizieren können, umfasst aufseiten des ersten Netzwerkelements die folgenden Schritte:
Bestimmen einer ersten Kanalinformation bezüglich des ersten Übertragungskanals basierend auf einem ersten Pilotsignal, das ein von dem Netzwerkknoten ausgesendetes, über den ersten Übertragungskanal übertragenes und von dem ersten Netzwerkelement empfangenes Signal repräsentiert; und
Ermitteln des kryptografischen Schlüssels unter Verwendung der ersten Kanalinformation und einer Information über eine kombinierte Kanalinformation, wobei die kombinierte Kanalinformation eine seitens des Netzwerkknotens basierend auf einem über den ersten Übertragungskanal von dem ersten Netzwerkelement zu dem Netzwerknoten übertragenen zweiten Pilotsignal und basierend auf einem über den zweiten Übertragungskanal von dem zweiten Netzwerkelement zu dem Netzwerknoten übertragenen dritten Pilotsignal bestimmte und an das erste Netzwerkelement übermittelte Kombination von Übertragungscharakteristiken des ersten und des zweiten Übertragungskanals repräsentiert.

[0008] Durch Ausführung der Schritte des Verfahrens kann ein kryptografischer Schlüssel erzeugt oder generiert werden. Bei den Netzwerkelementen kann es sich um Kommunikationseinrichtungen handeln, die jeweils ausgebildet sind, um Daten auszusenden und Daten zu empfangen. Beispielsweise kann das erste Netzwerkelement ausgebildet sein, um Daten über den ersten Übertragungskanal an den Netzwerknoten zu senden und Daten über den ersten Übertragungskanal von dem Netzwerknoten zu empfangen. Entsprechend kann das zweite Netzwerkele-

ment ausgebildet sein, um Daten über den zweiten Übertragungskanal an den Netzwerknoten zu senden und Daten über den zweiten Übertragungskanal von dem Netzwerknoten zu empfangen. Der Netzwerknoten kann ausgebildet sein, um von dem ersten Netzwerkelement empfangene Daten an das zweite Netzwerkelement weiterzuleiten. Entsprechend kann der Netzwerkknoten ausgebildet sein, um von dem zweiten Netzwerkelement empfangene Daten an das erste Netzwerkelement weiterzuleiten. Bei den Übertragungskanälen kann es sich jeweils um leitungsgebundene oder leitungslose Übertragungskanäle handeln. Dies beinhaltet auch optische Systeme mit einer Übertragung über Lichtwellenleiter, wie beispielsweise Glasfasern oder Plastikfasern. Ein Netzwerkelement kann beispielsweise Teil eines Sensors oder eines Aktors sein. Der Netzwerknoten kann Teil einer Steuervorrichtung zur Steuerung der Netzwerkelemente oder eines Routers bzw. Switches oder eine Weiterleitungseinrichtung sein. Die Netzwerkelemente können über den Netzwerkknoten miteinander kommunizieren. Um untereinander verschlüsselte Nachrichten austauschen zu können, können die Netzwerkelemente jeweils den gleichen kryptografischen Schlüssel erzeugen und für ein symmetrisches Verschlüsselungsverfahren nutzen. Nach Ermittlung der Schlüssel aufseiten beider Netzwerkelemente können die Netzwerkelemente weiterhin über den Netzwerkknoten oder beispielsweise über einen weiteren Netzwerkknoten oder direkt miteinander kommunizieren. Dabei können zwischen den Netzwerkelementen zu übertragende Daten mittels der Schlüssel auf der Senderseite verschlüsselt und auf der Empfängerseite entschlüsselt werden. Die Schlüssel können dabei so ermittelt worden sein, dass sie ausschließlich den beiden Netzwerkelementen bekannt sind. Auf diese Weise können zwischen den Netzwerkelementen zu übertragende Daten auch dann vor einer unerwünschten Entschlüsselung geschützt bleiben, wenn sie durch eine Abhöreinrichtung während der Übertragung abgehört werden.

[0009] Eine Kanalinformation kann beispielsweise eine physikalische Eigenschaft eines zugrunde liegenden Übertragungskanals definieren oder durch eine solche physikalische Eigenschaft definiert sein. Beispielsweise kann eine Kanalinformation eine Kanalimpulsantwort eines Übertragungskanals, eine Dämpfung eines Übertragungskanals, eine Phasenverschiebung einer Trägerfrequenz eines Übertragungskanals, eine Laufzeitverteilung bzw. delay spread eines Übertragungskanals sein oder einen oder mehrere andere geeignete charakteristische Kanalparameter darstellen. Bei den Pilotsignalen kann es sich um Signale handeln, die geeignet sind, um die Kanalinformation desjenigen Übertragungskanals zu ermitteln, über den die Pilotsignale übertragen werden. Beispielsweise kann ein Pilotsignal einem Dirac-Impuls oder einer Sprungfunktion nachempfunden sein. Als Pilotsignale eignen sich weiterhin z. B. so genannte „CAZAC-Sequenzen“ (Constant Amplitude Zero Autocorrelation), aber im Prinzip auch nahezu beliebige, dem Sender und Empfänger bekannte Datenfolgen. Die einzelnen Pilotsignale können gleichartig, beispielsweise identisch, oder unterschiedlich sein. Insbesondere kann das dritte Pilotsignal identisch zu dem zweiten Pilotsignal sein. Die Art der einzelnen Pilotsignale sollte dabei in der Regel den jeweiligen Empfängern bekannt sein, damit eine pilotbasierte Kanalschätzung durchgeführt werden kann.

[0010] Das zweite und das dritte Pilotsignal können zeitgleich ausgesendet werden oder den Netzwerknoten zeitgleich erreichen, sodass der Netzwerknoten das zweite und das dritte Pilotsignal in überlagerter Form empfangen kann. Der Netzwerkknoten kann dazu eine Empfangsschnittstelle zum Empfangen des zweiten Pilotsignals und des dritten Pilotsignals aufweisen. Der Netzwerkknoten kann ausgebildet sein, um die kombinierte Kanalinformation aus der empfangenen Überlagerung aus dem zweiten und dritten Pilotsignal zu bestimmen. Das erste Netzwerkelement kann diese kombinierte Kanalinformation vom Netzwerkknoten übermittelt bekommen.

[0011] Das Verfahren kann einen Schritt der synchronisierten Übertragung des zweiten Pilotsignals seitens des ersten Netzwerkelements umfassen. Dadurch kann eine synchrone Übertragung des zweiten Pilotsignals über den ersten Übertragungskanal und des dritten Pilotsignals über den zweiten Übertragungskanal ermöglicht werden. Auf diese Weise kann sichergestellt werden, dass das zweite und das dritte Pilotsignal in überlagerter Form von dem Netzwerkknoten empfangen werden und ein separater Empfang nicht möglich ist. Dies ist wichtig, damit der Netzwerkknoten selbst nicht die entsprechenden Schlüssel erzeugen kann, wodurch die Sicherheit erhöht wird. Dadurch wird der Netzwerkknoten daran gehindert, über das zweite und das dritte Pilotsignal die erste Kanalinformation und eine zweite Kanalinformation bezüglich des zweiten Übertragungskanals getrennt voneinander zu ermitteln. Das zweite Pilotsignal kann im Schritt des Bereitstellens an eine Schnittstelle zu dem ersten Übertragungskanal bereitgestellt werden oder über den ersten Übertragungskanal ausgesendet werden.

[0012] Beispielsweise kann im Schritt des synchronisierten Bereitstellens das zweite Pilotsignal ansprechend auf einen Empfang eines von dem Netzwerknoten ausgesendeten Auslösesignals bereitgestellt werden. Alternativ kann das zweite Pilotsignal eine vorbestimmte Zeitdauer nach einem Empfang des ersten Pilotsignals bereitgestellt werden. Dadurch kann der Netzwerkknoten auch auf das bevorstehende Eintreffen des zweiten und des dritten Pilotsignals vorbereitet werden.

[0013] Im Schritt des Ermittelns des kryptografischen Schlüssels kann aus der ersten Kanalinformation und der Information über die kombinierte Kanalinformation eine zweite Kanalinformation bezüglich des zweiten Übertragungskanals bestimmt werden. Der kryptografische Schlüssel kann unter Verwendung der ersten Kanalinformation und der zweiten Kanalinformation ermittelt werden. Somit kann die Information über die kombinierte Kanalinformation seitens des ersten Netzwerkelements genutzt werden, um die zweite Kanalinformation bezüglich des zweiten Übertragungskanals zu bestimmen, ohne dass das erste Netzwerkelement direkt mit dem zweiten Übertragungskanal gekoppelt ist. Zunächst wird nur ein kryptografischer Schlüssel ermittelt. Dadurch, dass beide Netzwerkelemente das gleiche Verfahren einsetzen, wird der Schlüssel dann schließlich auch symmetrisch, d. h., er kann in Verbindung mit symmetrischen Verschlüsselungsverfahren eingesetzt werden.

[0014] Ferner kann im Schritt des Ermittelns des kryptografischen Schlüssels basierend auf der ersten Kanalinformation und der zweiten Kanalinformation zumindest ein Kanalparameter bezüglich des ersten Übertragungskanals und/oder des zweiten Übertragungskanals bestimmt werden. Der kryptografische Schlüssel kann unter Verwendung des zumindest einen Kanalparameters ermittelt werden. Der zumindest eine Kanalparameter kann somit entweder dem ersten Übertragungskanal oder dem zweiten Übertragungskanal oder einem Verbund aus dem ersten und dem zweiten Übertragungskanal zugeordnet sein. Der zumindest eine Kanalparameter kann durch eine Verknüpfung der ersten Kanalinformation und der zweiten Kanalinformation bestimmt werden. Unterschiedliche Kanalparameter können durch unterschiedliche Verknüpfungen der ersten Kanalinformation und der zweiten Kanalinformation bestimmt werden. Eine Verknüpfung kann beispielsweise unter Verwendung einer Grundrechenart oder durch eine Faltung erfolgen.

[0015] Die aufseiten des ersten Netzwerkelements durchgeführten Schritte können in entsprechender Weise auch aufseiten des zweiten Netzwerkelements durchgeführt werden. Dabei können die aufseiten des zweiten Netzwerkelements durchgeführten Schritte, abgesehen von der auf die Aussendung des zweiten Pilotsignals abgestimmte Aussendung des dritten Pilotsignals, unabhängig von den aufseiten des ersten Netzwerkelements durchgeführten Schritten ausgeführt werden. Die jeweils eingesetzten Verfahren sind aber natürlich gleich, damit letzten Endes auch der gleiche Schlüssel auf beiden Seiten erzeugt wird. Es können also zwei Verfahren zur Ermittlung eines kryptografischen Schlüssels parallel aufseiten des ersten Netzwerkelements und des zweiten Netzwerkelements ausgeführt werden.

[0016] Somit kann das Verfahren oder ein aufseiten des zweiten Netzwerkelements separat ausgeführtes Verfahren die folgenden Schritte umfassen:
Bestimmen einer zweiten Kanalinformation bezüglich des zweiten Übertragungskanals basierend auf dem ersten Pilotsignal oder einem weiteren ersten Pilotsignal, das ein von dem Netzwerkknoten ausgesendetes, über den zweiten Übertragungskanal übertragenes und von dem zweiten Netzwerkelement empfangenes Signal repräsentiert; und
Ermitteln des kryptografischen Schlüssels unter Verwendung der zweiten Kanalinformation und der Information über die kombinierte Kanalinformation.

[0017] Ferner kann ein Verfahren zur Ermittlung eines kryptografischen Schlüssels in einem Netzwerk Schritte eines Verfahren zur Unterstützung einer Ermittlung von symmetrischen kryptografischen Schlüsseln in einem Netzwerk umfassen, die aufseiten des Netzwerkknotens ausgeführt werden.

[0018] Ein Verfahren zur Unterstützung einer Ermittlung von symmetrischen kryptografischen Schlüsseln in einem Netzwerk mit einem ersten Netzwerkelement, einem zweiten Netzwerkelement und einem Netzwerkknoten, wobei das erste Netzwerkelement über einen ersten Übertragungskanal und das zweite Netzwerkelement über einen zweiten Übertragungskanal mit dem Netzwerkknoten verbindbar sind, kann aufseiten des Netzwerkknotens die folgenden Schritte umfassen:
Aussenden eines ersten Pilotsignals über den ersten Übertragungskanal an das erste Netzwerkelement und des ersten Pilotsignals oder eines weiteren ersten Pilotsignals über den zweiten Übertragungskanal an das zweite Netzwerkelement;
Bestimmen einer kombinierten Kanalinformation bezüglich des ersten Übertragungskanals und des zweiten Übertragungskanals basierend auf einem zweiten Pilotsignal, das ein von dem ersten Netzwerkelement ausgesendetes, über den ersten Übertragungskanal übertragenes und von dem Netzwerkknoten empfangenes Signal repräsentiert, und basierend auf einem dritten Pilotsignal, das ein von dem zweiten Netzwerkelement ausgesendetes, über den zweiten Übertragungskanal übertragenes und von dem Netzwerkknoten empfangenes Signal repräsentiert; und
Aussenden einer Information über die kombinierte Kanalinformation an das erste Netzwerkelement und an das zweite Netzwerkelement, um dem ersten Netzwerkelement und dem zweiten Netzwerkelement die Ermittlung von symmetrischen kryptografischen Schlüsseln zu ermöglichen.

[0019] Die beiden ersten Pilotsignale können gleich sein. Alternativ können auch unterschiedliche Pilotsignale zur Kanalschätzung beim ersten und zweiten Netzwerkelement verwendet werden, d. h. das erste Pilotsignal und das weitere erste Pilotsignal können

sich voneinander unterscheiden, also beispielsweise unterschiedliche Datenfolgen aufweisen.

[0020] Somit können von dem ersten Netzwerkelement und dem zweiten Netzwerkelement unter Zusammenwirken der Netzwerkelemente und des Netzwerkknotens symmetrische Schlüssel erzeugt werden, die zur verschlüsselten Datenübertragung zwischen den Netzwerkelementen eingesetzt werden können. Dazu können zu übertragende Daten mithilfe des Schlüssels aufseiten des einen Netzwerkelements verschlüsselt werden, in verschlüsselter Form ausgesendet werden, von dem anderen Netzwerkelement in verschlüsselter Form empfangen und mithilfe des Schlüssels entschlüsselt werden.

[0021] Die vorliegende Erfindung schafft ferner eine oder mehrere Vorrichtungen, die ausgebildet ist oder sind, um die Schritte eines oder mehrerer erfindungsgemäßer Verfahren in entsprechenden Einrichtungen durchzuführen bzw. umzusetzen. Auch durch diese Ausführungsvariante der Erfindung in Form einer Vorrichtung kann die der Erfindung zugrunde liegende Aufgabe schnell und effizient gelöst werden.

[0022] Unter einer Vorrichtung kann vorliegend ein Netzwerkelement, ein Netzwerkknoten oder jeweils eine Teileinrichtung davon verstanden werden. Generell kann unter einer Vorrichtung ein elektrisches Gerät verstanden werden, das Eingangssignale empfangen oder einlesen und Ausgangssignale bereitstellen oder ausgeben kann. Eine Vorrichtung kann eine Schnittstelle aufweisen, die hard- und/oder softwaremäßig ausgebildet sein kann. Bei einer hardwaremäßigen Ausbildung können die Schnittstellen beispielsweise Teil eines sogenannten System-ASICs oder FPGAs sein, der verschiedenste Funktionen der Vorrichtung beinhaltet. Es ist jedoch auch möglich, dass die Schnittstellen eigene, integrierte Schaltkreise sind oder zumindest teilweise aus diskreten Bauelementen bestehen. Bei einer softwaremäßigen Ausbildung können die Schnittstellen Softwaremodule sein, die beispielsweise auf einem Mikrocontroller neben anderen Softwaremodulen vorhanden sind.

[0023] Von Vorteil ist auch ein Computerprogrammprodukt mit Programmcode, der auf einem maschinenlesbaren Träger wie einem Halbleiterspeicher, einem Festplattenspeicher oder einem optischen Speicher gespeichert sein kann und zur Durchführung des Verfahrens nach einer der vorstehend beschriebenen Ausführungsformen verwendet wird, wenn das Programmprodukt auf einem Computer oder einer Vorrichtung ausgeführt wird.

[0024] Der beschriebene Ansatz basiert auf einem symmetrischen Verfahren. Symmetrische Verfahren haben den Vorteil, dass Sie im Unterschied zu asymmetrischen Verfahren in der Regel eine niedrigere Rechenkomplexität aufweisen. Damit sind sie auch für leichtgewichtige Knoten, wie z. B. Sensoren, Aktoren, o.ä., geeignet, die üblicherweise nur über eine relativ geringe Rechenleistung verfügen und energieeffizient arbeiten sollen, beispielsweise aufgrund von Batteriebetrieb. Darüber hinaus steht oftmals nur eine begrenzte Bandbreite zur Datenübertragung zur Verfügung, was den Austausch von asymmetrischen Schlüsseln mit Längen von bis zu 2048 Bit, oder auch länger falls nötig, unattraktiv macht.

[0025] Bei symmetrischen Verfahren muss gewährleistet sein, dass sowohl Empfänger als auch Sender über den gleichen Schlüssel verfügen. Das zugehörige Schlüsselmanagement stellt dabei generell eine sehr anspruchsvolle Aufgabe dar. Im Bereich des Mobilfunks werden Schlüssel beispielsweise mithilfe von SIM-Karten in ein Mobiltelefon eingebracht und das zugehörige Netz kann dann der eindeutigen Kennung einer SIM-Karte den entsprechenden Schlüssel zuordnen. Im Fall von Wireless LANs hingegen erfolgt üblicherweise eine manuelle Eingabe der zu verwendenden Schlüssel, in der Regel durch die Eingabe eines Passwortes bei der Einrichtung eines Netzwerkes. Ein solches Schlüsselmanagement wird allerdings schnell sehr aufwendig und unpraktikabel, wenn eine sehr große Anzahl von Knoten vorhanden ist, beispielsweise in einem Sensornetzwerk oder anderen Maschine-zu-Maschine-Kommunikationssystemen. Durch den vorliegend beschriebenen Ansatz kann das Schlüsselmanagement vereinfacht werden. Beispielsweise wird dadurch eine Änderung der zu verwendenden Schlüssel oftmals mit geringem Aufwand möglich.

[0026] Der vorliegend beschriebene Ansatz kann auf einem unter dem Schlagwort „Physical Layer Security" bekannten Ansatz aufbauen, mithilfe dessen Schlüssel für symmetrische Verfahren automatisch auf der Grundlage der Übertragungskanäle zwischen den involvierten Knoten (Alice und Bob) erzeugt werden können. Dabei wird die Reziprozität dieser Übertragungskanäle ausgenutzt. Dies geschieht gemäß einer Ausführungsform wie folgt:
Beide Knoten schätzen eine bestimmte Anzahl von Kanalparametern, evtl. auch über die Zeit.

[0027] Diese Kanalparameter können von beiden Knoten geeignet quantisiert werden.

[0028] Mithilfe geeigneter Mechanismen kann dann ein Abgleich der quantisierten Kanalparameter unter Verwendung eines öffentlichen Protokolls erfolgen. Dies kann ggf. auch über den Netzwerkknoten erfolgen. Es kann zudem eine Validierung erfolgen, mithilfe derer sichergestellt werden kann, dass beide Netzwerkelemente tatsächlich denselben Schlüssel generiert haben. Dazu können z. B. geeignete Hash-Werte über die Schlüssel berechnet und ausgetauscht werden. Dies kann notwendig sein, da aufgrund von

Messungenauigkeiten, Rauschen, Interferenzen, etc. beide Knoten im Allgemeinen zunächst keine identischen Parametersätze ermittelt haben. Der Abgleich sollte dabei derart gestaltet sein, dass eine potenzielle Angreiferin (Eve), die die ausgetauschten Daten mithören kann, davon nicht ohne Weiteres auf die quantisierten Kanalparameter schließen kann. Auch der Netzwerkknoten sollte nicht in der Lage sein, entsprechende Rückschlüsse zu ziehen.

[0029] Auf der Grundlage der abgeglichenen, quantisierten Kanalparameter können schließlich entsprechende symmetrische Schlüssel erzeugt werden.

[0030] Da Eve mit genügend großem Abstand zu Alice und Bob (in der Größenordnung der sogenannten Kohärenzlänge, die bei den gängigen drahtlosen Kommunikationssystemen im Bereich von wenigen Zentimetern liegt) jeweils andere (unabhängige) Übertragungskanäle zu diesen Knoten sieht, kann sie nicht ohne Weiteres denselben Schlüssel rekonstruieren. Zudem kann mithilfe dieses Ansatzes auch ohne großen Aufwand regelmäßig ein Re-Keying durchgeführt werden, d. h. eine Neuberechnung der zu verwendenden Schlüssel, und es muss nicht auf komplexe, rechenintensive asymmetrische Verfahren zurückgegriffen werden.

[0031] Der beschriebene Ansatz bietet folglich unter anderem den Vorteil der Kosteneinsparung und des geringeren Energieverbrauchs im Vergleich zu asymmetrischen Verfahren. Zudem wird ein stark vereinfachtes Schlüsselmanagement im Vergleich zu (herkömmlichen) symmetrischen Verfahren ermöglicht. Es besteht eine einfache Einsetzbarkeit, auch für technikaverse Personen („Plug-and-Secure"). Ferner ist eine skalierbare Sicherheit gegeben, d. h. es können je nach Anforderung im Prinzip Schlüssel beliebiger Länge erzeugt werden und es ist eine Skalierbarkeit des Systems gegeben.

[0032] Der vorliegend beschriebene Ansatz umfasst ein Verfahren, mit dem auch in Fällen mit einem relativ schlechten Signal-zu-Rauschverhältnis (SNR) zwischen Alice und Bob oder falls diese gar nicht direkt miteinander kommunizieren können eine effiziente automatisierte Generierung entsprechender symmetrischer Schlüssel möglich ist. Dies geschieht unter Zuhilfenahme eines dazwischen liegenden weiteren Knotens, z. B. ein Relay, im Weiteren als Max bezeichnet, der sowohl zu Alice als auch zu Bob ein deutlich besseres SNR hat als das SNR zwischen Alice und Bob selbst. Max unterstützt dabei Alice und Bob bei der Schlüsselgenerierung auf geeignete Art und Weise, ohne den Schlüssel selbst ohne Weiteres rekonstruieren zu können.

[0033] Ein solches Verfahren kann auch dann noch sinnvoll eingesetzt werden, wenn die im ersten Schritt des als „Physical Layer Security" bekannten Ansatzes ermittelten Kanalparameter mit Rauschen, Messungenauigkeiten, Interferenzen, etc. keine ausreichend hohe Korrelation aufweisen. In einem solchen Fall kann die Generierung entsprechender Schlüssel gemäß dem vorliegend beschriebenen Ansatz dennoch sehr schnell durchgeführt werden, da kein erhöhter Aufwand für den Abgleich der Parameter erforderlich ist und das System daher schwer angreifbar ist. Dies gilt insbesondere auch dann, wenn das Signal-zu-Rauschverhältnis zwischen Alice und Bob relativ schlecht ist bzw. eine direkte Kommunikation zwischen diesen Knoten gar nicht möglich ist, also z. B. bei einem relativ großen Abstand zwischen beiden Knoten, bei dazwischen liegenden Wänden oder anderen Objekten, etc.

[0034] Gemäß dem vorliegend beschriebenen Ansatz können Alice und Bob zunächst jeder für sich den Kanal zu Max schätzen und anschließend Max den Summenkanal von Alice und Bob zusammen, oder umgekehrt. Je nach Ausprägung genügt es auch schon, einzelnen Kenngrößen oder Charakteristika zu schätzen und zur Schlüsselgenerierung zu verwenden. Es ist nicht unbedingt erforderlich, die komplette Impulsantwort oder Übertragungsfunktion zu schätzen. Dies gilt auch für die folgenden Ausführungen in diesem Absatz. Diese Summenkanalinformation kann dann mithilfe eines öffentlichen Protokolls an Alice und Bob übertragen werden, die somit unter Ausnutzung der Kenntnis ihres eigenen Kanals zu Max die entsprechenden Kanäle zwischen Max und dem jeweiligen anderen Knoten ermitteln können. Folglich kennen sowohl Alice als auch Bob die jeweiligen Kanäle zwischen diesen Knoten und Max und können diese auf geeignete Art und Weise miteinander kombinieren, um auf der Grundlage der kombinierten Kanalinformation schließlich entsprechende symmetrische Schlüssel abzuleiten. Max sowie potenzielle Angreifer hingegen kennen ggf. nur den geschätzten bzw. mithilfe des öffentlichen Protokolls übertragenen Summenkanal, nicht aber die zugehörigen Einzelkanäle zu Alice und Bob, sodass diese nicht ohne Weiteres in der Lage sind, die generierten symmetrischen Schlüssel zu rekonstruieren.

[0035] Wesentliche Vorteile des vorliegend beschriebenen Ansatzes sind eine automatisierte, effiziente Generierung von symmetrischen kryptografischen Schlüsseln basierend auf physikalischen Kanälen, mit allen zuvor bereits kurz beschriebenen Vorteilen, die auch dann möglich ist, falls keine direkte Kommunikation zwischen den involvierten Knoten (Alice und Bob) möglich ist oder falls ein vergleichsweise schlechtes SNR vorliegt. Dabei wird ausgenutzt, dass in praktischen Systemen oftmals ohnehin der dafür benötigte Hilfsknoten (Max) vorhanden ist. Bei einem Kommunikationssystem mit zentralisiertem Medienzugriff, wie beispielsweise bei einem Pollingverfahren, kann diese Rolle die zentrale Steuerungseinheit übernehmen (z.B. ein soge-

nannter „Master“-Knoten) wohingegen bei Multihop-Übertragungen im Rahmen von drahtlosen Kommunikationssystemen wie ZigBee (basierend auf IEEE 802.15.4) oder Wireless LANs die ohnehin involvierten Relaystationen die entsprechende Funktionalität mit realisieren können. Ein potenzieller Angreifer (Eve), der nur die mithilfe des öffentlichen Protokolls übertragene Kanalinformation, beispielsweise eine Summenkanalinformation mitbekommt, kann nicht ohne Weiteres Rückschlüsse auf die zugehörigen Einzelkanäle ziehen und somit die automatisch generierten symmetrischen Schlüssel ermitteln. Das gleiche gilt auch für den Hilfsknoten (Max) selbst. Bei der Kanalinformation muss es sich im Allgemeinen nicht unbedingt um die Summe handeln, sondern lediglich um eine geeignete Kombination der einzelnen Kanalparameter.

[0036] Mit einer mehrmaligen Anwendung des beschriebenen Verfahrens ist prinzipiell eine Ende-zu-Ende-Verschlüsselung oder zumindest die Absicherung über mehrere Links möglich. Mit den herkömmlicherweise betrachteten Verfahren werden symmetrische Schlüssel immer nur für genau einen Link erzeugt und auch nur auf diesem Link angewendet.

[0037] Im Vergleich zu herkömmlichen Schlüsselmanagementverfahren oder asymmetrischen Ansätzen kann zudem jederzeit problemlos ein Re-Keying durchgeführt werden, um auf diese Weise den Schutzgrad weiter zu erhöhen.

[0038] Die Erfindung wird nachstehend anhand der beigefügten Zeichnungen beispielhaft näher erläutert. Es zeigen:

[0039] Fig. 1 eine schematische Darstellung eines Netzwerks gemäß einem Ausführungsbeispiel der vorliegenden Erfindung;

[0040] Fig. 2 eine schematische Darstellung eines Netzwerkelements gemäß einem Ausführungsbeispiel der vorliegenden Erfindung;

[0041] Fig. 3 eine schematische Darstellung eines Netzwerkknotens gemäß einem Ausführungsbeispiel der vorliegenden Erfindung; und

[0042] Fig. 4 ein Ablaufdiagramm eines Gesamtverfahrens zur Ermittlung symmetrischer kryptografischer Schlüssel in einem Netzwerk gemäß einem Ausführungsbeispiel der vorliegenden Erfindung.

[0043] In der nachfolgenden Beschreibung bevorzugter Ausführungsbeispiele der vorliegenden Erfindung werden für die in den verschiedenen Figuren dargestellten und ähnlich wirkenden Elemente gleiche oder ähnliche Bezugszeichen verwendet, wobei auf eine wiederholte Beschreibung dieser Elemente verzichtet wird.

[0044] Fig. 1 zeigt eine schematische Darstellung eines Netzwerks gemäß einem Ausführungsbeispiel der vorliegenden Erfindung. Gezeigt ist ein Netzwerk mit einem ersten Netzwerkelement **102**, einem zweiten Netzwerkelement **104** und einem Netzwerkknoten **106**. Das erste Netzwerkelement **102** wird auch als Alice, das zweite Netzwerkelement **104** auch als Bob und der Netzwerkknoten **106** auch als Max bezeichnet. Generell können die Netzwerkelemente **102**, **104** und der Netzwerkknoten **106** auch allgemein als Knoten bezeichnet werden.

[0045] Das erste Netzwerkelement **102** kann über einen ersten Übertragungskanal **112** mit dem Netzwerkknoten **106** kommunizieren, es können also Daten zwischen dem ersten Netzwerkelement **102** und dem Netzwerkknoten **106** über den ersten Übertragungskanal **112** übertragen werden. Das zweite Netzwerkelement **104** ist über einen zweiten Übertragungskanal **114** mit dem Netzwerkknoten **106** verbunden, es können also Daten zwischen dem zweiten Netzwerkelement **104** und dem Netzwerkknoten **106** über den zweiten Übertragungskanal **112** übertragen werden. Der Netzwerknoten **106** kann ausgebildet sein, um von dem ersten Netzwerkelement **102** empfangene Daten an das zweite Netzwerkelement **104** weiterzuleiten und umgekehrt. Auf diese Weise können die Netzwerkelemente **102**, **104** über den Netzwerkknoten **106** miteinander kommunizieren.

[0046] Die Übertragungskanäle **112**, **114** können an sich abhörbar ausgeführt sein. Beispielsweise kann eine Datenübertragung über die Übertragungskanale **112**, **114** gemäß einem öffentlich bekannten Protokoll, bzw. Übertragungsverfahren erfolgen. Werden über die Übertragungskanale **112**, **114** Daten unverschlüsselt übermittelt, so können diese beispielsweise von einem weiteren Netzwerkelement oder einer Abhöreinrichtung **120**, auch als Eve bezeichnet, abgehört und genutzt werden. Dazu kann die Abhöreinrichtung **120** über einen dritten Übertragungskanal **122**, einem sogenannten Abhörkanal mit dem ersten Netzwerkknoten **102**, dem ersten Übertragungskanal **112** oder dem Netzwerkknoten **106** gekoppelt sein und zusätzlich oder alternativ über einen vierten Übertragungskanal **124**, einem sogenannten Abhörkanal mit dem zweiten Netzwerkknoten **104**, dem zweiten Übertragungskanal **114** oder dem Netzwerkknoten **106** gekoppelt sein.

[0047] Um eine sichere Datenübertragung zwischen den Netzwerkelementen **102**, **104** über die Übertragungskanäle **112**, **114** und den Netzwerkknoten **106** zu ermöglichen, können die Netzwerkelemente **102**, **104** ein symmetrisches Verschlüsselungsverfahren einsetzen. Das symmetrische Verschlüsselungsverfahren basiert auf zwei symmetrischen, also gleichen kryptografischen Schlüsseln, von denen jeweils einer von den beiden Netzwerkelementen **102**, **104** erzeugt und zum Verschlüsseln von über die Übertragungs-

kanäle **112**, **114** zu übertragenden Daten und zum Entschlüsseln von über die Übertragungskanäle **112**, **114** übertragenen Daten verwendet werden können.

[0048] Gemäß diesem Ausführungsbeispiel sind die Netzwerkelemente **102**, **104** jeweils ausgebildet, um den Schlüssel basierend auf Kanalinformationen bezüglich der Übertragungskanäle **112**, **114** zu bestimmen. Bei den Kanalinformationen kann es sich beispielsweise um eine Kanalimpulsantwort $h_1(t)$ bezüglich des ersten Übertragungskanals **112**, und um eine Kanalimpulsantwort $h_2(t)$ bezüglich des zweiten Übertragungskanals **114** handeln. Anstelle der Kanalimpulsantwort $h_1(t)$, $h_2(t)$ kann es sich bei den Kanalinformationen aber auch um andere geeignete Parameter oder charakteristische Werte der Übertragungskanäle **112**, **114** handeln.

[0049] Im Folgenden wird eine Erzeugung der Schlüssel durch die Netzwerkelemente **102**, **104** anhand eines Ausführungsbeispiels beschrieben.

[0050] Dazu wird eine Anordnung betrachtet, wie sie in **Fig.** 1 dargestellt ist. Die zwei Netzwerkelemente **102**, **104** (Alice und Bob), bei denen es sich um zwei Knoten eines Netzwerks handeln kann, wollen Daten sicher übertragen und hierzu ein geeignetes symmetrisches Verschlüsselungsverfahren einsetzen. Das SNR des direkten Kanals zwischen den Netzwerkelementen **102**, **104** (Alice und Bob) ist ggf. allerdings relativ schlecht oder es ist überhaupt keine direkte Kommunikation zwischen den beiden Netzwerkelementen **102**, **104** möglich. Daher gibt es einen dazwischen liegenden Netzwerkknoten **106**, bei dem es sich um eine Hilfsstation (Max) handeln kann und der ein besseres SNR zu sowohl zu dem ersten Netzwerkelement **102** (Alice) als auch zu dem zweiten Netzwerkelement **104** (Bob) aufweiset. Der Netzwerkknoten **106** kann in praktischen Realisierungen beispielsweise ein Relay sein, eine zentrale Steuerungseinheit oder aber ein beliebiger anderer Knoten. Darüber hinaus ist in **Fig.** 1 auch noch eine potenzielle Angreiferin **120** (Eve) dargestellt, die die zwischen den Netzwerkelementen **102**, **104** (Alice und Bob) ausgetauschten Daten abhören möchte.

[0051] In **Fig.** 1 sind für jeden Link **112**, **114**, **122**, **124** auch die entsprechenden Kanalimpulsantworten $h_1(t)$, $h_2(t)$, $h_3(t)$, $h_4(t)$ eingezeichnet, die die zugehörigen Übertragungskanäle **112**, **114**, **122**, **124** zu einem bestimmten Zeitpunkt vollständig beschreiben. Im Folgenden wird ein Ausführungsbeispiel der vorliegenden Erfindung derart beschrieben, dass symmetrische kryptografische Schlüssel basierend auf diesen Kanalimpulsantworten $h_1(t)$, $h_2(t)$, $h_3(t)$, $h_4(t)$ erzeugt werden und diese daher auch entsprechend geschätzt oder anderweitig ermittelt werden müssen. Prinzipiell ist es aber auch denkbar, dass nur bestimmte, auch unvollständige Kanalinformationen, z. B. der Betrag der Dämpfung oder die Phasenverschiebung auf verschiedenen Unterträgern eines OFDM-Systems oder der Delay-Spread zwischen zwei Knoten, beispielsweise jeweils zwischen dem Netzwerknoten **106** und den Netzwerkelementen **102**, **104** dafür verwendet werden. Zudem können selbstverständlich auch Sequenzen davon betrachtet werden, d. h. beispielsweise eine ganze Reihe von Kanalimpulsantworten $h_1(t)$, $h_2(t)$, $h_3(t)$, $h_4(t)$ oder eben andere, gegebenenfalls unvollständige Kanalinformationen, z. B. zu verschiedenen Zeitpunkten.

[0052] Das vorgeschlagene Verfahren funktioniert dabei gemäß einem Ausführungsbeispiel wie folgt: Von dem Netzwerkknoten **106** (Max) werden Pilotsignale ausgesendet, auf deren Grundlage die Netzwerkelemente **102**, **104** (Alice und Bob) die Kanalimpulsantworten $h_1(t)$ und $h_2(t)$ schätzen können.

[0053] Die Netzwerkelemente **102**, **104** (Alice und Bob) senden daraufhin gleichzeitig ebenfalls geeignete Pilotsignale. Das Senden dieser Signale kann dabei beispielsweise durch das Senden einer speziellen Nachricht von dem Netzwerkknoten **106** (Max) angestoßen werden oder implizit nach einer vordefinierten Zeit nach dem Senden der Pilotsignale von dem Netzwerkknoten **106** (Max). Da der Netzwerkknoten **106** (Max) folglich nur eine Überlagerung der Pilotsignale von den Netzwerkelemente **102**, **104** (Alice und Bob) empfängt, kann er nur die Summe der Kanalimpulsantworten $h_1(t) + h_2(t)$ schätzen. Es ist nicht ohne Weiteres möglich, daraus dann die einzelnen Kanalimpulsantworten $h_1(t)$ und $h_2(t)$ zu ermitteln.

[0054] Der Netzwerkknoten **106** (Max) signalisiert die Summe der Kanalimpulsantworten $h_1(t) + h_2(t)$ mithilfe eines öffentlichen Protokolls an die Netzwerkelemente **102**, **104** (Alice und Bob). Diese Information über die Summe der Kanalimpulsantworten $h_1(t) + h_2(t)$ kann prinzipiell auch von der Abhöreinrichtung **120** (Eve) empfangen werden, aber aufgrund der bereits erwähnten Schwierigkeit, daraus $h_1(t)$ und $h_2(t)$ abzuleiten, stellt dies kein größeres Problem dar.

[0055] Da das erste Netzwerkelement **102** (Alice) die Kanalimpulsantwort $h_1(t)$ und das zweite Netzwerkelement **104** (Bob) die Kanalimpulsantwort $h_2(t)$ kennt, können beide Netzwerkelemente **102**, **104** (Alice und Bob) die jeweils andere Kanalimpulsantwort $h_2(t)$ respektive $h_1(t)$ aus der Summe $h_1(t) + h_2(t)$ ermitteln.

[0056] Die Netzwerkelemente **102**, **104** (Alice und Bob) sind ausgebildet, um dann $h_1(t)$ und $h_2(t)$ auf geeignete Art und Weise zu kombinieren und so einen gemeinsamen Satz von Kanalparametern zu ermitteln. Hierbei sind prinzipiell verschiedene Verknüpfungsfunktionen denkbar, wie z. B. die Faltung beider Funktionen $h_1(t)$ und $h_2(t)$, die Multiplikation oder ähnliches. Die Verknüpfung der Kanalimpulsantwor-

ten $h_1(t)$ und $h_2(t)$ sollte insbesondere derart erfolgen, dass das Ergebnis der Verknüpfung nicht ohne Weiteres aus der Summe der Kanalimpulsantworten $h_1(t) + h_2(t)$ ermittelt werden kann.

[0057] Der gemeinsame Satz von Kanalparametern dient dann als Grundlage zur Generierung entsprechender symmetrischer kryptografischer Schlüssel mithilfe einer bekannten prinzipiellen Vorgehensweise, d. h. mit dem Abgleich der im Allgemeinen zunächst noch unterschiedlichen Kanalparametersätze mit einem geeigneten (öffentlichen) Protokoll und der sich daran anschließenden Erzeugung der eigentlichen Schlüssel sowie der Validierung der erzeugten Schlüssel, beispielsweise durch den Austausch geeigneter Hash-Werte, die auf der Grundlage dieser Schlüssel berechnet worden sind. Somit können die beiden Netzwerkelemente **102**, **104** jeweils getrennt voneinander aus einer Verknüpfung der Kanalimpulsantworten $h_1(t)$ und $h_2(t)$ jeweils einen Satz von Kanalparametern ermitteln. Die beiden ermittelten Sätze von Kanalparametern können dann gegeneinander abgeglichen werden, um in beiden Netzwerkelementen **102**, **104** jeweils einen abgeglichenen Satz von Kanalparametern zu erhalten, aus denen dann wiederum von beiden Netzwerkelementen **102**, **104** getrennt voneinander die Schlüssel generiert werden können.

[0058] Da die potenzielle Angreiferin **120** (Eve) bei genügend großem Abstand zu dem Netzwerkknoten **106** (Max), der üblicherweise in der Größenordnung von wenigen Zentimetern liegt, andere Kanalimpulsantworten $h_3(t)$, $h_4(t)$ zu den Netzwerkelementen **102**, **104** (Alice und Bob) sieht als der Netzwerkknoten **106** (Max) und selbst bei Kenntnis der Summe $h_1(t) + h_2(t)$ nicht ohne Weiteres die Einzelkanalimpulsantworten $h_1(t)$ und $h_2(t)$ bestimmen kann, ist die potenzielle Angreiferin **120** (Eve) nicht der Lage, selbst die von den Netzwerkelementen **102**, **104** erzeugten Schlüssel zu ermitteln.

[0059] Darüber hinaus ist zu beachten, dass bei einer späteren Datenübertragung von den Netzwerkelementen **102**, **104** (Alice zu Bob) oder andersherum mit Einbeziehung des Netzwerkknotens **106** (Max) dieser ggf. ebenfalls die entsprechenden Kanalimpulsantworten $h_1(t)$, $h_2(t)$ dem ersten Netzwerkelement **102** bzw. dem zweiten Netzwerkelement **104** (Alice bzw. Bob) schätzen muss. Falls zwischen der Schlüsselgenerierung und der eigentlichen Datenübertragung aber genügend Zeit vergeht, üblicherweise in der Größenordnung der Kohärenzzeit der Kanäle, die bei drahtlosen Systemen meist weniger als eine Sekunde beträgt, sind die Kanalimpulsantworten zu diesem Zeitpunkt allerdings unabhängig von den zuvor bestimmten Kanalimpulsantworten $h_1(t)$, $h_2(t)$, weshalb der Netzwerkknoten **106** (Max) selbst damit dann nicht nachträglich auf die generierten Schlüssel schließen kann.

[0060] Ein generelles Sicherheitsrisiko würde natürlich bestehen, falls der Netzwerkknoten **106** (Max) korrumpiert ist. Sofern das Versenden der Pilotsignale durch die Netzwerkelemente **102**, **104** (Alice und Bob) aber mithilfe einer speziellen Nachricht von dem Netzwerkknoten **106** (Max) angestoßen wird, die immer an beide Netzwerkelemente **102**, **104** geht, kann insbesondere in drahtlosen oder busbasierten Kommunikationssystemen sichergestellt werden, dass beide Netzwerkelemente **102**, **104** immer wirklich gleichzeitig ihre Pilotsignale übertragen und der Netzwerkknoten **106** (Max) somit nur die Summe der Einzelkanalimpulsantworten $h_1(t)$, $h_2(t)$ schätzen kann. Dem Netzwerkknoten **106** (Max) wäre es folglich nicht ohne Weiteres möglich, den Netzwerkelementen **102**, **104** (Alice und Bob) eine reguläre Funktionsweise vorzutäuschen und somit später ggf. vertrauliche Nachrichten abzufangen. Was natürlich aber nicht verhindert werden kann, ist eine Unterbindung der Schlüsselgenerierung durch den Netzwerkknoten **106** (Max), was von den Netzwerkelementen **102**, **104** (Alice und Bob) aber entsprechend festgestellt werden könnte.

[0061] Das beschriebene Verfahren kann in einer Anordnung mit Netzwerkelementen **102**, **104** in Form von Knoten eingesetzt werden, die dynamisch unter Einbeziehung des Netzwerkknotens **106** symmetrische kryptografische Schlüssel erzeugen wollen, und von einer potenziellen Angreiferin **220** bedroht sein können. Die in **Fig.** 1 gezeigten Funktionen hi(t)(i = 1, ..., 4) bezeichnen die einzelnen Kanalimpulsantworten der verschiedenen Links zu dem betrachteten Zeitpunkt.

[0062] Das Netzwerk kann weitere nicht gezeigte Netzwerkelemente oder Netzwerkknoten aufweisen. Beispielsweise kann das zweite Netzwerkelement **104** über einen weiteren Netzwerkknoten mit einem dritten Netzwerkelement gekoppelt sein. Zur Kommunikation zwischen dem zweiten und dem dritten Netzwerkelement können in entsprechender Weise erzeugte Schlüssel generiert werden.

[0063] **Fig.** 2 zeigt eine schematische Darstellung eines Netzwerkelements **102** gemäß einem Ausführungsbeispiel der vorliegenden Erfindung. Dabei kann es sich um eines der in **Fig.** 1 gezeigten Netzwerkelemente handeln, das in einem Netzwerk über einen ersten Übertragungskanal **112** mit einem Netzwerkknoten und weiter über einen zweiten Übertragungskanal mit einem weiteren Netzwerkelement kommunizieren kann.

[0064] Das Netzwerkelement **102** weist eine Kommunikationsschnittstelle **230** zur leitungslosen oder leitungsgebundenen Kommunikation mit einem von dem Netzwerkelement **102** entfernt angeordneten Netzwerkknoten über den ersten Übertragungskanal **112** auf. Das Netzwerkelement **102** ist ausgebildet,

um über die Kommunikationsschnittstelle **230** ein erstes Pilotsignal zu empfangen und über die Kommunikationsschnittstelle **230** ein zweites Pilotsignal auszusenden. Ferner ist das Netzwerkelement **102** ausgebildet, um über die Kommunikationsschnittstelle **230** Daten zu empfangen, die eine Information über eine kombinierte Kanalinformation bezüglich des ersten Übertragungskanals **112** und des zweiten Übertragungskanals umfasst.

[0065] Das Netzwerkelement **102** weist ferner eine Bestimmungseinrichtung **232** auf. Die Bestimmungseinrichtung **232** ist ausgebildet, um das von der Kommunikationsschnittstelle **230** empfangene erste Pilotsignal zu verwenden, um eine erste Kanalinformation bezüglich des ersten Übertragungskanals **112** zu bestimmen. Dazu kann der Bestimmungseinrichtung **232** eine Information über eine Charakteristik des von dem Netzwerkknoten ausgesendeten ersten Pilotsignals vorliegen.

[0066] Ferner weist das Netzwerkelement **102** eine Ermittlungseinrichtung **234** auf. Die Ermittlungseinrichtung **234** ist ausgebildet, um die erste Kanalinformation und die von der Kommunikationsschnittstelle **230** empfangene Information über die kombinierte Kanalinformation zu verwenden, um eine zweite Kanalinformation bezüglich des zweiten Übertragungskanals zu bestimmen. Ferner ist die Ermittlungseinrichtung **234** ausgebildet, um die erste Kanalinformation und die zweite Kanalinformation zu verwenden, um einen symmetrischen kryptografischen Schlüssel zu ermitteln. Alternativ kann die Ermittlungseinrichtung **234** ausgebildet sein, um den Schlüssel direkt aus der ersten Kanalinformation und der Information über die kombinierte Kanalinformation zu ermitteln.

[0067] Die Ermittlungseinrichtung **234** kann ausgebildet sein, um basierend auf der Kanalinformation und der Information über die kombinierte Kanalinformation einen oder mehrere Kanalparameter bezüglich eines Übertragungskanals zwischen dem Netzwerkelement **102** und dem weiteren Netzwerkelement zu bestimmen und den oder die Kanalparameter zur Ermittlung des Schlüssels zu verwenden. Der Kanalparameter kann von einer physikalischen Eigenschaft der des ersten Übertragungskanals **112** und des zweiten Übertragungskanals abhängig sein und somit ein individuelles Merkmal der Übertragungskanäle zwischen den Netzwerkelementen darstellen.

[0068] Um den oder die Kanalparameter mit einem oder mehreren parallel dazu von dem weiteren Netzwerkelement bestimmten Kanalparametern abgleichen zu können, kann die Ermittlungseinrichtung **234** ausgebildet sein, um eine geeignete Abgleichinformation über die Kommunikationsschnittstelle **230** an das weitere Netzwerkelement zu senden und/oder eine geeignete Abgleichinformation über die Kommunikationsschnittstelle **230** von dem weiteren Netzwerkelement zu empfangen.

[0069] Ferner weist das Netzwerkelement **102** eine Verschlüsselungseinrichtung **236** auf. Die Verschlüsselungseinrichtung **236** ist ausgebildet, um an das weitere Netzwerkelement zu übertragende Daten zu empfangen, mit dem von der Ermittlungseinrichtung **234** ermittelten Schlüssel zu verschlüsseln und als verschlüsselte Daten an die Kommunikationsschnittstelle **230** zur Aussendung der verschlüsselten Daten bereitzustellen. Bei den zu übertragende Daten kann es sich beispielsweise um erfasste Sensordaten handeln, wenn das Netzwerkelement **102** Teil eines Sensors ist.

[0070] Ferner weist das Netzwerkelement **102** eine Entschlüsselungseinrichtung **238** auf. Die Entschlüsselungseinrichtung **238** ist ausgebildet, um von der Kommunikationsschnittstelle **230** empfangene verschlüsselte Daten zu empfangen und unter Verwendung des von der Ermittlungseinrichtung **234** ermittelten Schlüssels zu entschlüsseln und als entschlüsselte Daten zur weiteren Übertragung oder weiteren Nutzung bereitzustellen.

[0071] Das weitere Netzwerkelement, über das das Netzwerkelement **102** über den Netzwerkknoten kommunizieren kann, kann entsprechend zu dem Netzwerkelement **102** ausgeführt sein und ausgebildet sein, um einen entsprechenden symmetrischen kryptografischen Schlüssel zu ermitteln.

[0072] Das Netzwerkelement **102** kann beispielsweise ein Sensor oder ein Aktor sein. Demnach können über die verschlüsselten Daten beispielsweise Messwerte, Sensorwerte, Zustandsinformationen oder Steuerinformationen in verschlüsselter Form übertragen werden. Es kann sich bei den verschlüsselten Daten also um Nutzdaten handeln, die innerhalb des Netzwerkes übertragen werden.

[0073] **Fig.** 3 zeigt eine schematische Darstellung eines Netzwerkknotens **106** gemäß einem Ausführungsbeispiel der vorliegenden Erfindung. Dabei kann es sich um den in **Fig.** 1 gezeigten Netzwerkknoten handeln, der in einem Netzwerk über einen ersten Übertragungskanal **112** mit einem ersten Netzwerkelement und über einen zweiten Übertragungskanal **114** mit einem zweiten Netzwerkelement kommunizieren kann.

[0074] Der Netzwerkknoten **106** weist eine Kommunikationsschnittstelle **340** zur leitungslosen oder leitungsgebundenen Kommunikation mit den Netzwerkelementen über den ersten Übertragungskanal **112** und den zweiten Übertragungskanal auf. Alternativ kann der Netzwerkknoten **106** auch zwei Kommunikationsschnittstellen besitzen – eine für den ersten Übertragungskanal **112** und eine für den zweiten

Übertragungskanal **114**. Der Netzwerkknoten **106** ist ausgebildet, um über die Kommunikationsschnittstelle **340** ein erstes Pilotsignal auszusenden und über die Kommunikationsschnittstelle **340** eine Überlagerung von Pilotsignalen zu empfangen, die synchronisiert von den Netzwerkelementen ausgesendet werden. Ferner ist die Kommunikationsschnittstelle **340** ausgebildet, um eine Information über eine kombinierte Kanalinformation bezüglich des ersten Übertragungskanals **112** und des zweiten Übertragungskanals **114** auszusenden.

[0075] Der Netzwerkknoten **106** weist ferner eine Bestimmungseinrichtung **342** auf. Die Bestimmungseinrichtung **342** ist ausgebildet, um die von der Kommunikationsschnittstelle **340** empfangene Überlagerung von Pilotsignalen der Netzwerkelemente zu verwenden, um eine kombinierte Kanalinformation bezüglich des ersten Übertragungskanals **112** und des zweiten Übertragungskanals **114** zu bestimmen und an die Kommunikationsschnittstelle **340** zur Übertragung an die Netzwerkelemente bereitzustellen.

[0076] Die Kommunikationsschnittstelle **340** ist ferner ausgebildet, um über den ersten Übertragungskanal **112** von dem ersten Netzwerkelement empfangene verschlüsselte Daten zu empfangen und durch Aussenden über den zweiten Übertragungskanal **114** an das zweite Netzwerkelement weiterzuleiten. Entsprechend ist die Kommunikationsschnittstelle **340** ausgebildet, um über den zweiten Übertragungskanal **112** von dem zweiten Netzwerkelement empfangene verschlüsselte Daten zu empfangen und durch Aussenden über den ersten Übertragungskanal **114** an das erste Netzwerkelement weiterzuleiten. Dabei werden die verschlüsselten Daten jeweils ohne zwischengeschaltete Entschlüsselung weitergeleitet.

[0077] **Fig.** 4 zeigt ein mögliches Ablaufdiagramm eines Gesamtverfahrens zur Ermittlung symmetrischer kryptografischer Schlüssel in einem Netzwerk gemäß einem Ausführungsbeispiel der vorliegenden Erfindung. Bei dem Netzwerk kann es sich beispielsweise um das in **Fig.** 1 gezeigte Netzwerk mit einem ersten Netzwerkelement, einem zweiten Netzwerkelement und einem Netzwerkknoten handeln. Das Gesamtverfahren kann Schritte von zwei auf den Netzwerkelementen parallel ausgeführten Verfahren zur Ermittlung eines symmetrischen kryptografischen Schlüssels und Schritte eines auf dem Netzwerkknoten ausgeführten Verfahren zur Unterstützung einer Ermittlung von symmetrischen kryptografischen Schlüsseln in einem Netzwerk umfassen.

[0078] In einem aufseiten des Netzwerkknotens ausgeführten Schritt **451** wird von dem Netzwerkknoten zumindest ein Pilotsignal an die Netzwerkelemente ausgesendet.

[0079] In einem aufseiten des ersten Netzwerkelements ausgeführten Schritt **453** wird das Pilotsignal von dem ersten Netzwerkelement empfangen und zur Bestimmung einer ersten Kanalinformation bezüglich eines ersten Übertragungskanals zwischen dem ersten Netzwerkelement und dem Netzwerkknoten verwendet. In einem aufseiten des zweiten Netzwerkelements ausgeführten Schritt **455** wird das Pilotsignal von dem zweiten Netzwerkelement empfangen und zur Bestimmung einer zweiten Kanalinformation bezüglich eines zweiten Übertragungskanals zwischen dem zweiten Netzwerkelement und dem Netzwerkknoten verwendet. Die Schritte **453**, **455** können parallel ausgeführt werden.

[0080] In einem aufseiten des ersten Netzwerkelements ausgeführten Schritt **457** wird ein weiteres Pilotsignal von dem ersten Netzwerkelement ausgesendet. Synchronisiert dazu wird in einem aufseiten des zweiten Netzwerkelements ausgeführten Schritt **459** wird ein weiteres Pilotsignal von dem zweiten Netzwerkelement ausgesendet.

[0081] In einem aufseiten des Netzwerkknotens ausgeführten Schritt **461** wird eine Überlagerung der weiteren von den Netzwerkelementen ausgesendeten Pilotsignale empfangen und zur Bestimmung einer kombinierten Kanalinformation bezüglich des ersten und des zweiten Übertragungskanals verwendet. In einem weiteren Schritt **463** wird eine Information über die kombinierte Kanalinformation von dem Netzwerkknoten an die Netzwerkelemente ausgesendet.

[0082] In einem aufseiten des ersten Netzwerkelements ausgeführten Schritt **465** wird die Information über die kombinierte Kanalinformation von dem ersten Netzwerkelement empfangen und zusammen mit der ersten Kanalinformation zur Ermittlung eines symmetrischen kryptografischen Schlüssels verwendet. In entsprechender Weise wird in einem aufseiten des zweiten Netzwerkelements ausgeführten Schritt **467** die Information über die kombinierte Kanalinformation von dem zweiten Netzwerkelement empfangen und zusammen mit der zweiten Kanalinformation zur Ermittlung eines dem in dem ersten Netzwerkelement entsprechenden weiteren symmetrischen kryptografischen Schlüssel verwendet.

[0083] Die in den beiden Netzwerkelementen ermittelten Schlüssel sind gemäß diesem Ausführungsbeispiel identisch.

[0084] Die beiden Schlüssel können nach ihrer Ermittlung zur Kommunikation zwischen den Netzwerkelementen unter Einsatz eines symmetrischen Verschlüsselungsverfahrens eingesetzt werden. Dabei kann die Kommunikation weiterhin über den Netzwerkknoten oder über einen anderen Übertragungskanal, beispielsweise über einen direkt zwischen den Netzwerkelementen verlaufenden Übertragungska-

nal oder über einen über einen oder mehrere andere Netzwerkknoten verlaufenden Übertragungskanal erfolgen.

[0085] Anhand der vorangegangenen Figuren wurde ein Verfahren zur Erzeugung symmetrischer kryptografischer Schlüssel basierend auf physikalischen Kanälen **112**, **114** unter Einbeziehung eines Netzwerkknotens **106** beschrieben, der eine Hilfsstation darstellen kann.

[0086] Das Verfahren eignet sich zur automatischen Generierung von symmetrischen kryptografischen Schlüsseln basierend auf physikalischen Kanälen **112**, **114** in drahtlosen oder drahtgebundenen Kommunikationssystemen. Damit können ohne hohen Aufwand symmetrische Verschlüsselungsverfahren zur Wahrung der Vertraulichkeit von zu übertragenden Daten eingesetzt werden, was insbesondere für die Anwendung im Bereich der Maschine-zu-Maschine Kommunikation, also z. B. für die Übertragung von Daten zwischen verschiedenen Netzwerkelementen **102**, **104** beispielsweise in Form von Sensorknoten und/oder Aktorknoten, interessant ist, die im Allgemeinen nur über sehr begrenzte Ressourcen verfügen und ggf. nicht mit vertretbarem Aufwand manuell im Feld konfiguriert werden können..

[0087] Das Verfahren kann die Kommunikation zwischen mehreren Knoten **102**, **104**, **106** eines Kommunikationssystems betreffen, die ggf. von unterschiedlichen Herstellern stammen können. Zur Durchführung der Schritte des Verfahrens können zwischen verschiedenen Knoten **102**, **104**, **106** Nachrichten und Signale entsprechend einem verwendeten Protokoll ausgetauscht werden.

[0088] Der beschriebene Ansatz zur automatisierten Generierung symmetrischer kryptografischer Schlüssel kann bei einer Vielzahl von drahtlosen und drahtgebundenen Kommunikationssystemen eingesetzt werden. Der beschriebene Ansatz ist jedoch nicht auf solche Systeme beschränkt, sondern kann allgemein in Kommunikationssystemen mit zumindest zwei Teilnehmern und zumindest einem Zwischenknoten eingesetzt werden. Beispielsweise kann der beschriebene Ansatz in sämtlichen Anwendungen des Internets eingesetzt werden, also beispielsweise in der Heim- und Gebäudeautomatisierung, der Telemedizin, in Car-to-X-Systemen oder der industriellen Automatisierungstechnik.

[0089] Die beschriebenen und in den Figuren gezeigten Ausführungsbeispiele sind nur beispielhaft gewählt. Unterschiedliche Ausführungsbeispiele können vollständig oder in Bezug auf einzelne Merkmale miteinander kombiniert werden. Auch kann ein Ausführungsbeispiel durch Merkmale eines weiteren Ausführungsbeispiels ergänzt werden. Ferner können erfindungsgemäße Verfahrensschritte wiederholt sowie in einer anderen als in der beschriebenen Reihenfolge ausgeführt werden. Umfasst ein Ausführungsbeispiel eine „und/oder“-Verknüpfung zwischen einem ersten Merkmal und einem zweiten Merkmal, so ist dies so zu lesen, dass das Ausführungsbeispiel gemäß einer Ausführungsform sowohl das erste Merkmal als auch das zweite Merkmal und gemäß einer weiteren Ausführungsform entweder nur das erste Merkmal oder nur das zweite Merkmal aufweist.

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 Nicht-Patentliteratur

- IEEE 802.15.4 [0035]

Patentansprüche

1. Verfahren zur Ermittlung eines kryptografischen Schlüssels in einem Netzwerk mit einem ersten Netzwerkelement (**102**), einem zweiten Netzwerkelement (**104**) und einem Netzwerkknoten (**106**), wobei das erste Netzwerkelement über einen ersten Übertragungskanal (**112**) und das zweite Netzwerkelement über einen zweiten Übertragungskanal (**114**) mit dem Netzwerkknoten kommunizieren kann, wobei das Verfahren aufseiten des ersten Netzwerkelements die folgenden Schritte umfasst:
Bestimmen (**453**) einer ersten Kanalinformation bezüglich des ersten Übertragungskanals basierend auf einem ersten Pilotsignal, das ein von dem Netzwerkknoten ausgesendetes, über den ersten Übertragungskanal übertragenes und von dem ersten Netzwerkelement empfangenes Signal repräsentiert; und
Ermitteln (**465**) des kryptografischen Schlüssels unter Verwendung der ersten Kanalinformation und einer Information über eine kombinierte Kanalinformation, wobei die kombinierte Kanalinformation eine seitens des Netzwerkknotens basierend auf einem über den ersten Übertragungskanal von dem ersten Netzwerkelement zu dem Netzwerknoten übertragenen zweiten Pilotsignal und basierend auf einem über den zweiten Übertragungskanal von dem zweiten Netzwerkelement zu dem Netzwerknoten übertragenen dritten Pilotsignal bestimmte und an das erste Netzwerkelement übermittelte Kombination von Übertragungscharakteristiken des ersten und des zweiten Übertragungskanals repräsentiert.

2. Verfahren gemäß Anspruch 1, mit einem Schritt der synchronisierten Übertragung (**457**) des zweiten Pilotsignals seitens des ersten Netzwerkelements (**102**), um eine synchrone Übertragung des zweiten Pilotsignals über den ersten Übertragungskanal (**112**) und des dritten Pilotsignals über den zweiten Übertragungskanal (**114**) zu ermöglichen.

3. Verfahren gemäß Anspruch 2, bei dem im Schritt der synchronisierten Übertragung (**453**) das zweite Pilotsignal ansprechend auf einen Empfang eines von dem Netzwerkknoten (**106**) ausgesendeten Auslösesignals oder eine vorbestimmte Zeitdauer nach einem Empfang des ersten Pilotsignals bereitgestellt wird.

4. Verfahren gemäß einem der vorangegangenen Ansprüche, bei dem im Schritt des Ermittelns (**465**) des kryptografischen Schlüssels, aus der ersten Kanalinformation und der Information über die kombinierte Kanalinformation eine zweite Kanalinformation bezüglich des zweiten Übertragungskanals (**112**) bestimmt wird und der kryptografische Schlüssel unter Verwendung der ersten Kanalinformation und der zweiten Kanalinformation ermittelt wird.

5. Verfahren gemäß Anspruch 4, bei dem im Schritt des Ermittelns des kryptografischen Schlüssels, basierend auf der ersten Kanalinformation und der zweiten Kanalinformation zumindest ein Kanalparameter bezüglich des ersten Übertragungskanals (**112**) und/oder des zweiten Übertragungskanals (**114**) bestimmt wird und der kryptografische Schlüssel unter Verwendung des zumindest einen Kanalparameters ermittelt wird.

6. Verfahren gemäß einem der vorangegangenen Ansprüche, bei dem es sich bei den Kanalinformationen um Kanalimpulsantworten ($h_1(t)$, $h_2(t)$) handelt.

7. Verfahren gemäß einem der vorangegangenen Ansprüche, das aufseiten des zweiten Netzwerkelements (**104**) die folgenden Schritte umfasst:
Bestimmen (**459**) einer zweiten Kanalinformation bezüglich des zweiten Übertragungskanals (**114**) basierend auf dem ersten Pilotsignal oder einem weiteren ersten Pilotsignal, das ein von dem Netzwerkknoten (**106**) ausgesendetes, über den zweiten Übertragungskanal übertragenes und von dem zweiten Netzwerkelement empfangenes Signal repräsentiert; und
Ermitteln (**467**) des kryptografischen Schlüssels unter Verwendung der zweiten Kanalinformation und der Information über die kombinierte Kanalinformation.

8. Verfahren gemäß einem der vorangegangenen Ansprüche, das aufseiten des Netzwerkknotens (**106**) die folgenden Schritte des Verfahrens gemäß Anspruch 9 umfasst.

9. Verfahren zur Unterstützung einer Ermittlung von symmetrischen kryptografischen Schlüsseln in einem Netzwerk mit einem ersten Netzwerkelement (**102**), einem zweiten Netzwerkelement (**104**) und einem Netzwerkknoten (**106**), wobei das erste Netzwerkelement über einen ersten Übertragungskanal (**112**) und das zweite Netzwerkelement über einen zweiten Übertragungskanal (**114**) mit dem Netzwerkknoten kommunizieren kann, wobei das Verfahren aufseiten des Netzwerkknotens die folgenden Schritte umfasst:
Aussenden (**451**) eines ersten Pilotsignals über den ersten Übertragungskanal an das erste Netzwerkelement und des ersten Pilotsignals oder eines weiteren ersten Pilotsignals über den zweiten Übertragungskanal an das zweite Netzwerkelement;
Bestimmen (**461**) einer kombinierten Kanalinformation bezüglich des ersten Übertragungskanals und des zweiten Übertragungskanals basierend auf einem zweiten Pilotsignal, das ein von dem ersten Netzwerkelement ausgesendetes, über den ersten Übertragungskanal übertragenes und von dem Netzwerkknoten empfangenes Signal repräsentiert, und basierend auf einem dritten Pilotsignal, das ein von dem zweiten Netzwerkelement ausgesendetes, über den zweiten Übertragungskanal übertragenes und

von dem Netzwerkknoten empfangenes Signal repräsentiert; und
Aussenden (**463**) einer Information über die kombinierte Kanalinformation an das erste Netzwerkelement und an das zweite Netzwerkelement, um dem ersten Netzwerkelement und dem zweiten Netzwerkelement die Ermittlung von symmetrischen kryptografischen Schlüsseln zu ermöglichen.

10. Vorrichtung (**102**, **104**, **106**), die ausgebildet ist, um die Schritte zumindest eines Verfahrens gemäß einem der Ansprüche 1 bis 9 durchzuführen.

11. Computer-Programmprodukt mit Programmcode zur Durchführung zumindest eines Verfahrens nach einem der Ansprüche 1 bis 9, wenn das Programmprodukt auf einer Vorrichtung ausgeführt wird.

Es folgen 2 Seiten Zeichnungen

Anhängende Zeichnungen

Fig. 1

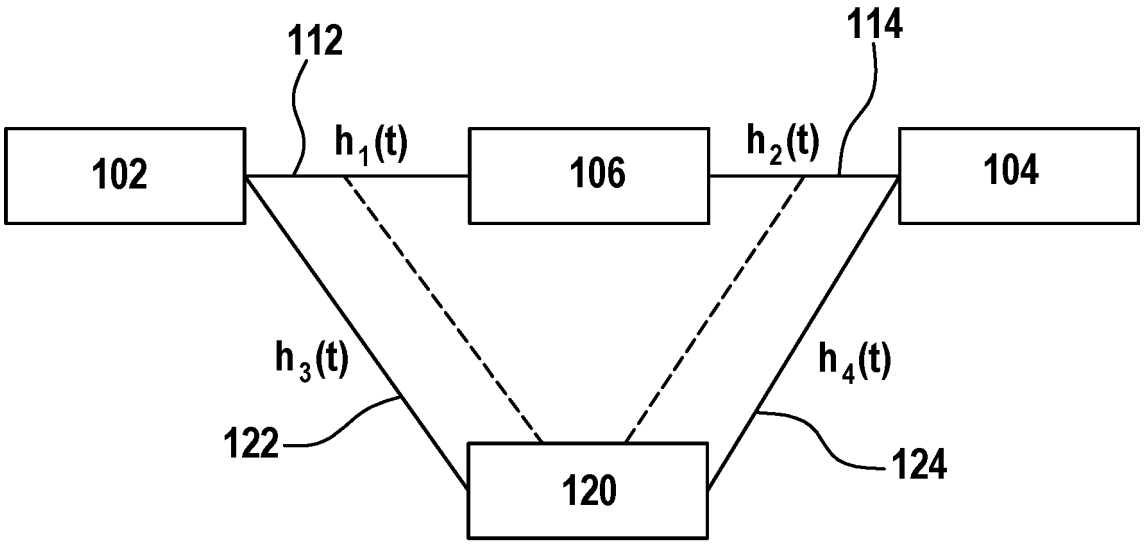


Fig. 2

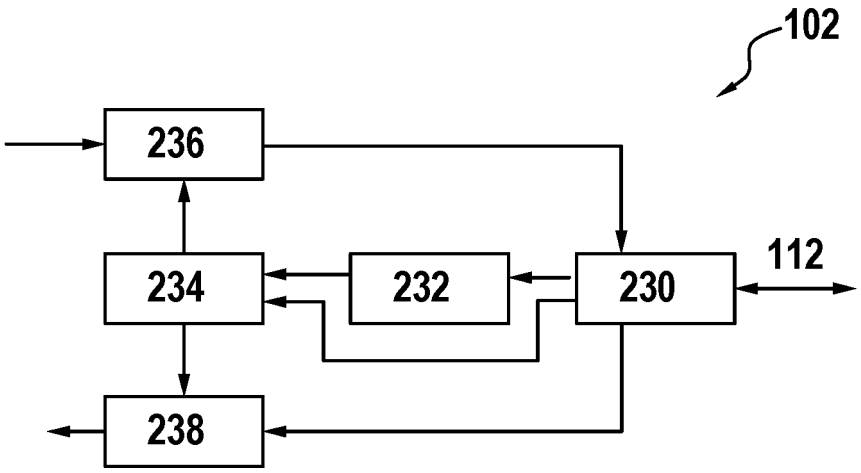


Fig. 3

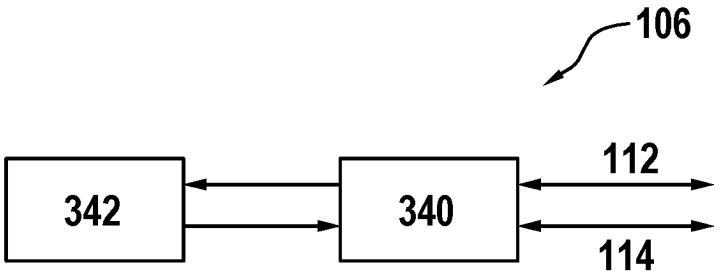


Fig. 4