(19) Deutsches Patent- und Markenamt

(10) **DE 10 2014 212 219 A1** 2015.12.31

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2014 212 219.8**
(22) Anmeldetag: **25.06.2014**
(43) Offenlegungstag: **31.12.2015**

(51) Int Cl.: ***H04L 9/32*** (2006.01)

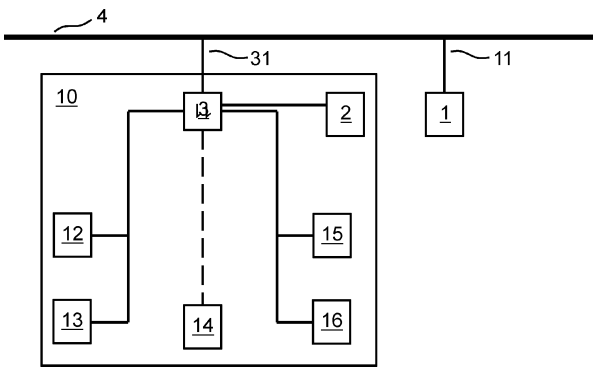
(71) Anmelder:
Robert Bosch GmbH, 70469 Stuttgart, DE

(72) Erfinder:
Guajardo Merchan, Jorge, Pittsburgh, Pann., US; Duplys, Paulius, 71706 Markgröningen, DE; Guillaume, Rene, 40489 Düsseldorf, DE; Zibuschka, Jan, 36124 Eichenzell, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren zur Authentifizierung und Anbindung eines Geräts an ein Netzwerk sowie hierzu eingerichteter Teilnehmer des Netzwerks**

(57) Zusammenfassung: Die Erfindung geht aus von einem Verfahren zur gegenseitigen Authentifizierung eines Geräts und eines Teilnehmers eines Netzwerks und zur Anbindung des Geräts an das Netzwerk durch den Teilnehmer. Hierzu empfängt der Teilnehmer von einem Nutzerendgerät eine erste Identifikationsinformation über das anzubindende Gerät sowie eine Aufforderung, das Gerät an das Netzwerk anzubinden. Der bindet Teilnehmer das Gerät an das Netzwerk an, indem es eine verschlüsselte Kommunikationsverbindung mit ihm aufbaut. Das Gerät und der Teilnehmer authentifizieren sich über die verschlüsselte Kommunikationsverbindung unter Verwendung der ersten Identifikationsinformation gegenseitig.



Beschreibung

[0001] Die vorliegende Erfindung betrifft Verfahren zur Authentifizierung und Anbindung eines Geräts an ein Netzwerk sowie einen Netzwerkteilnehmer und ein Computerprogramm, die dazu eingerichtet sind, alle Schritte eines der Verfahren durchzuführen.

Stand der Technik

[0002] Eine sichere Kommunikation zwischen verschiedenen Geräten wird in einer zunehmend vernetzten Welt immer wichtiger und stellt in vielen Anwendungsbereichen eine wesentliche Voraussetzung für die Akzeptanz und somit auch den wirtschaftlichen Erfolg der entsprechenden Anwendungen dar. Dies umfasst – je nach Anwendung – verschiedene Schutzziele, wie beispielsweise die Wahrung der Vertraulichkeit der zu übertragenden Daten, die gegenseitige Authentifizierung der beteiligten Knoten oder die Sicherstellung der Datenintegrität.

[0003] Zur Erreichung dieser Schutzziele kommen üblicherweise geeignete kryptographische Verfahren zum Einsatz, die man generell in zwei verschiedene Kategorien unterteilen kann: Symmetrische Verfahren, bei denen Sender und Empfänger über denselben kryptographischen Schlüssel verfügen, sowie asymmetrische Verfahren, bei denen der Sender die zu übertragenden Daten mit dem öffentlichen (d.h. auch einem potenziellen Angreifer möglicherweise bekannten) Schlüssel des Empfängers verschlüsselt, die Entschlüsselung aber nur mit dem zugehörigen privaten Schlüssel erfolgen kann, der idealerweise nur dem Empfänger bekannt ist.

[0004] Asymmetrische Verfahren haben unter anderem den Nachteil, dass sie in der Regel eine sehr hohe Rechenkomplexität aufweisen. Damit sind sie nur bedingt für ressourcenbeschränkte Knoten, wie z.B. Sensoren, Aktoren, o.ä., geeignet, die üblicherweise nur über eine relativ geringe Rechenleistung sowie geringen Speicher verfügen und energieeffizient arbeiten sollen, beispielsweise aufgrund von Batteriebetrieb oder dem Einsatz von Energy Harvesting. Darüber hinaus steht oftmals nur eine begrenzte Bandbreite zur Datenübertragung zur Verfügung, was den Austausch von asymmetrischen Schlüsseln mit Längen von 2048 Bit oder noch mehr unattraktiv macht.

[0005] Bei symmetrischen Verfahren hingegen 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 mit Hilfe 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 drahtlosen lokalen Netzwerken hingegen erfolgt üblicherweise eine manuelle Eingabe der zu verwendenden Schlüssel (in der Regel durch die Eingabe eines Passwortes) bei der Einrichtung eines Netzwerkes. Dies setzt allerdings voraus, dass das anzubindende Gerät über eine entsprechende Nutzerschnittstelle verfügt. Viele Geräte, die zukünftig (oft massenweise) in die lokalen Netzwerke des „Internet der Dinge“ angebunden werden sollen, wie beispielsweise Sensoren und Aktoren, haben aus Platz- und Kostengründen keine solche Schnittstelle.

[0006] Die meisten heute eingesetzten Lösungen zur Anbindung integrierter Bauteile wie Sensoren und Aktoren, die über keine eigene Bedienschnittstelle verfügen, an lokale Netzwerke, beispielsweise in der Heimautomatisierung, bieten nur wenig Sicherheit gegen böswillige Eindringlinge in das lokale Netzwerk. Typischerweise setzt der Nutzer das zentrale Gateway in einen bestimmten Betriebsmodus, in dem es aktiv nach neuen Geräten sucht, z.B. nach Sensoren oder Aktoren, und jedes gefundene, neue Gerät dem Netzwerk hinzufügt. Es werden also alle in der Suchphase detektierten Geräte als vertrauenswürdig eingestuft. Das ermöglicht Angreifern, schadhafte Knoten an das lokale Netzwerk anzubinden. Selbst wenn es sich bei den unerwünscht angebundenen Knoten (z.B. bei der Heimautomatisierung Knoten aus einer Nachbarwohnung) nicht um schadhafte Knoten handelt, kann die Anbindung zu einem Eingriff in die Privatsphäre führen.

[0007] Ziel ist dagegen eine sichere Anbindung, welche die Integrität und Vertraulichkeit der im Netzwerk verteilten Daten sowie die Authentizität der Daten und der am Netzwerk beteiligte Netzwerkknoten sicherstellt.

[0008] Neben der Sicherheit ist eine weitere Anforderung an die Anbindung solcher Geräte an lokale Netzwerke, dass diese schnell und einfach erfolgen kann, auch durch technisch nicht sehr versierte Nutzer.

[0009] Verfahren zur Absicherung von Sensordaten gegen Manipulation und die Sicherstellung einer Transaktionsauthentifizierung, z.B. in einem Kraftfahrzeugnetzwerk, mit Hilfe gängiger Verschlüsselungsverfahren sind z.B. in der DE 10 2009 002 396 A1 und in der DE 10 2009 045 133 A1 offenbart.

[0010] In der Veröffentlichung ‘B. Clifford Neuman and Theodore Ts'o: "Kerberos: An Authentication Service for Computer Networks", IEEE Communications 32 (9): 33–8. doi:10.1109/35.312841, September 1994’ wird ein Authentifizierungsverfahren für Netzwerke offenbart.

Offenbarung der Erfindung

[0011] Die Erfindung betrifft Verfahren gemäß den unabhängigen Verfahrensansprüchen sowie ein Computerprogramm und einen Netzwerkteilnehmer, die dazu eingerichtet sind, eines der Verfahren durchzuführen. Ausgegangen wird dabei vorteilhafterweise von dem Einsatz einer Identifikationsinformation zur Unterstützung der Authentifizierung und der sicheren Anbindung eines Geräts, welchem die Identifikationsinformation zugeordnet ist, an ein Netzwerk.

[0012] Diese Identifikationsinformation kann als Basis für eine gegenseitige Authentifizierung des anzubindenden Geräts und eines Teilnehmers des Netzwerks dienen. Sie wird hierzu von einem Nutzerendgerät mit einer ersten Aufforderung, das Gerät an das Netzwerk anzubinden, an den Netzwerkteilnehmer gesendet. Der Teilnehmer bindet dann das Gerät an das Netzwerk an, indem es eine verschlüsselte Kommunikationsverbindung mit ihm aufbaut, insbesondere über eine gemeinsame Schlüsselaushandlung mit dem Gerät. Über diese verschlüsselte Kommunikationsverbindung kann dann die gegenseitige Authentisierung unter Verwendung der ersten Identifikationsinformation erfolgen.

[0013] Durch die Verknüpfung einer verschlüsselten Kommunikation mit einer nur schwer manipulierbaren Authentifizierung auf Basis einer über ein vertrauenswürdiges Nutzerendgerät empfangenen Identifikationsinformation wird eine sichere Anbindung eines Knotens ermöglicht. Diese ist nur schwer manipulierbar und kommt ohne hohen Hardwareaufwand und ohne aufwendige Verwaltung geheimer Information (z.B. über eine zentrale Infrastruktur) aus. Nutzerendgeräte wie Smartphones, Tablets, Notebooks, PCs verfügen bereits über große Hardwareressourcen können, insbesondere durch die geeignete Software, leicht für den Einsatz in einem solchen Verfahren angepasst werden.

[0014] Bei dem Netzwerkteilnehmer kann es sich vorzugsweise um ein Gateway eines lokalen Netzwerks handeln. Dieses verknüpft das Netzwerk mit dem Internet und verfügt damit bereits über die Ressourcen für typische Sicherheitsmechanismen, wie sie für die Internetkommunikation nötig sind. Auch ein solches Gateway kann somit leicht für den Einsatz in einem solchen Verfahren angepasst werden.

[0015] Um das Gesamtverfahren noch sicherer gegen Manipulation oder das Abhören durch Angreifer zu machen, verfügen das Nutzerendgerät und der Teilnehmer vorteilhafterweise über eine abgesicherte Kommunikationsverbindung und haben sich bereits im Vorfeld gegenseitig authentifiziert.

[0016] Eine besonders sichere gegenseitige Authentifizierung zwischen Netzwerkteilnehmer und Gerät erfolgt in einer bevorzugten Ausgestaltung, indem die Identifikationsinformation über das Gerät mit Zufallszahlen verknüpft wird. Dabei können Nachrichten auf ausgetauscht werden, die verschlüsselt Zufallszahlen und die Identifikationsinformation enthalten. Auf Basis des gemeinsamen Geheimnisses, nämlich der Identifikationsinformation, und der Verifizierung des richtigen Kommunikationspartners über dessen Abgleich und den Abgleich von hin und her übertragenen Zufallszahlen, kann dann die gegenseitige Authentifizierung erfolgen.

[0017] Noch weiter absichern lässt sich das Verfahren, indem die Zufallszahlen und die Identifikationsinformationen nicht lediglich verschlüsselt übertragen werden, sondern Abbildungen, insbesondere Streuwertfunktionen, über Zufallszahlen und Identifikationsinformationen gebildet werden und diese verschlüsselt übertragen werden. In diesem Fall erfolgt die Authentifizierung dann aufgrund eines Vergleichs der entschlüsselten Abbildungen mit in den beteiligten Knoten selbst entsprechend gebildeten Abbildungen.

[0018] In einer alternativen Ausgestaltung kann eine zweite Identifikationsinformation über den Netzwerkteilnehmer zusätzlich zur ersten Identifikationsinformation über das Gerät als Basis für die gegenseitige Authentifizierung dienen. Hierbei verfügt das Gerät über diese zweite Identifikationsinformation und übermittelt diese, insbesondere wiederum verknüpft mit Zufallszahlen, an den Netzwerkteilnehmer. Dieses Verfahren ist durch die Verwendung von zwei geteilten Geheimnissen noch sicherer, dafür besteht ein entsprechend etwas erhöhter Verwaltungsaufwand.

[0019] In einer weiteren alternativen Ausgestaltung kann die Identifikationsinformation über das Gerät von dem Teilnehmer und dem Gerät dazu herangezogen werden, einen gemeinsamen Nachrichtenauthentifizierungscode (MAC) zu generieren und auf dessen Basis die gegenseitige Authentifizierung und gegebenenfalls auch abgesicherte Kommunikation zu erreichen.

Zeichnungen

[0020] Nachfolgend ist die Erfindung unter Bezugnahme auf die beiliegenden Zeichnungen und anhand von Ausführungsbeispielen näher beschrieben. Dabei zeigen

[0021] Fig. 1 schematisch ein beispielhaftes Netzwerk mit Internetverbindung und Nutzerendgeräte, die an das Internet bzw. an das Netzwerk angeschlossen sind,

[0022] Fig. 2 schematisch einen beispielhaften Ablauf eines Verfahrens zur Authentifizierung zwischen

einem Gerät und dem Teilnehmer eines Netzwerks sowie Anbindung des Geräts an das Netzwerk.

Beschreibung der Ausführungsbeispiele

[0023] Es wird erwartet, dass das viel beschriebene „Internet der Dinge“ aus mehreren Milliarden integrierten Geräten besteht, die untereinander in einem gemeinsamen, öffentlichen Netzwerk verbunden sind, wie es Computer und Server im heutigen Internet sind. Eine große Anzahl der „Dinge“ werden Sensoren und Aktoren sein, die mit einem Internetfähigen Gateway verbunden sind und mit diesem ein lokales Netzwerk bilden. Die Teilnehmer bzw. Netzwerkknoten eines solchen Netzwerkes können mittels kabelgebundener, funkgestützter, optischer oder sonstiger Kommunikation Daten austauschen.

[0024] Ein Beispiel eines solchen lokalen Netzwerks ist die Verknüpfung von Sensoren und Aktoren für die Heimautomatisierung (Smart Home). Ein solches lokales Netzwerk wird typischerweise von Privatpersonen betrieben. Auf das zentrale Gateway kann von einem PC oder einem mobilen Endgerät aus über das Internet zugegriffen werden. Der Nutzer kann somit aus der Entfernung Informationen aus dem lokalen Netzwerk erhalten und dieses kontrollieren. Das Nutzerendgerät (PC, Smartphone, Tablet, Notebook etc.) und das Gateway eines solchen Netzwerks verfügen dabei gewöhnlicherweise bereits über eine ausreichende Rechenleistung, um zum Beispiel kryptographische Verfahren wie PKI-Verfahren oder die Erzeugung eines eigenen Paars aus privatem und öffentlichem Schlüssel zu erzeugen. Sensor- und Aktorknoten in einem lokalen Netzwerk verfügen in der Regel nicht über vergleichbare Hardwareressourcen.

[0025] In **Fig.** 1 ist schematisch ein beispielhaftes lokales Netzwerk **10** gezeigt. Das Netzwerk **10** ist sternförmig aufgebaut und weist ein zentrales Gateway **3** auf. An das Netzwerk **10** angebunden, d.h. abgesichert mit dem Netzwerk **10** kommunizierend, sind die Teilnehmer / Netzwerkknoten **12**, **13**, **15** und **16**. Dabei kann es sich z.B. bei den Teilnehmern **12** und **13** sowie **15** und **16** jeweils um ein Sensor-Aktor-Paar handeln. Mit **14** ist ein neu an das Netzwerk **10** anzubindendes Gerät bezeichnet. Während die Verbindungen von **12**, **13**, **15** und **16** zum zentralen Gateway **3** bereits abgesichert sind (dargestellt durch durchgezogene Verbindunglinien), kann das anzubindende Gerät **14** zwar mit dem zentralen Netzwerk kommunizieren, die Kommunikationsverbindung ist allerdings noch nicht abgesichert (durch gestrichelte Verbindungslinie angedeutet). Abgesichert bedeutet hier die Sicherstellung von mindestens einem von: Integrität der kommunizierten Daten, Vertraulichkeit der kommunizierten Daten, der Authentizität der Teilnehmer. So kann beispielweise bei einer Anwendung von Sensoren im Medizinbereich die Vertraulichkeit der Daten im Vordergrund stehen, während bei einer Anwendung zur Eindringlingserkennung die Integrität der Daten von besonderer Bedeutung ist oder bei der Ansteuerung einer Heizungsanlage die Authentizität der Ansteuerdaten entscheidend ist.

[0026] Weiterhin in **Fig.** 1 gezeigt sind Nutzerendgeräte **1** und **2**. Hierbei kann es sich beispielsweise um Rechner wie Desktop-PCs handeln oder um mobile Endgeräte wie Smartphones, Notebooks oder Tablets. Das Nutzerendgerät **1** weist eine Verbindung **11** zum Internet **4** auf. Auch das zentrale Gateway **3** des Netzwerks **10** weist eine Verbindung **31** zum Internet **4** auf. Eine Kommunikation zwischen Nutzerendgerät **1** und Gateway **3** kann somit über das Internet erfolgen. Nutzerendgerät **2** ist über das lokale Netzwerk **10** mit dem zentralen Gateway verbunden und kann so mit diesen kommunizieren.

[0027] Für die Authentifizierung eines neuen Geräts (beispielsweise eines Sensors oder Aktors) in einem Netzwerk und die Anbindung des neuen Geräts an das Netzwerk soll ein Nutzerendgerät eingesetzt werden, welches mit dem Netzwerk verbunden ist. Um die Sicherheit des Verfahrens zu gewährleisten weisen ein Teilnehmer des Netzwerks (bei dem es sich vorzugsweise um ein Gateway des Netzwerks handelt) und das Nutzerendgerät vorzugsweise eine sichere Kommunikationsverbindung auf und sind vorzugsweise gegenseitig authentifiziert.

[0028] Zur weiteren Absicherung der Kommunikation zwischen Netzwerkteilnehmer und Nutzerendgerät kann unter Ausnutzung einer bereits bestehenden sicheren Kommunikationsverbindung eine Initialisierungsphase zwischen dem Nutzerendgerät und dem Teilnehmer erfolgen. Während dieser Initialisierung erzeugen sowohl das Nutzerendgerät als auch der Netzwerk-Teilnehmer jeweils ihr eigenes (einzigartiges) Schlüsselpaar aus öffentlichem und privatem Schlüssel. Das Nutzerendgerät fordert den Teilnehmer auf, ein Zertifikat für den öffentlichen Schlüssel des Nutzerendgeräts zu erstellen. Hierzu sendet es eine entsprechende Anforderung (CSR: Certificate Signing Request) an den Teilnehmer, welche den öffentlichen Schlüssel des Nutzerendgeräts enthält. Der Netzwerkteilnehmer sendet ein signiertes Zertifikat an das Nutzerendgerät und schließt damit die Initialisierungsphase ab.

[0029] Die Anbindung eines neuen Knoten oder Geräts an das Netzwerk kann erfolgen, wie in **Fig.** 2 gezeigt.

[0030] Der Informationsaustausch in der beschriebenen Initialisierungsphase ist in **Fig.** 2 in den Schritten **201** und **202** dargestellt.

[0031] Der Netzwerkteilnehmer **3** empfängt vom Nutzerendgerät **1** oder **2** (im folgenden **1**, **2**) in Schritt **204** eine Identifikationsinformation über das anzubin-

dende Gerät **14**. Die Identifikationsinformation kann das Nutzerendgerät **1**, **2** dabei direkt aus dem Gerät **14** ausgelesen haben (sofern zwischen den beiden eine sichere bzw. vertrauenswürdige Kommunikationsschnittstelle besteht), wie durch Schritt **203** angedeutet. Alternativ kann das Nutzerendgerät **1**, **2** die Identifikationsinformation auch optisch ausgelesen haben, beispielsweise von einem Barcode oder einem QR-Code, z.B. von einer Oberfläche des Geräts **14**, dessen Verpackung, dessen Gebrauchsanweisung oder sonstigen Begleitdokumenten. Auch kann das Nutzerendgerät **1**, **2** die Identifikationsinformation über das Internet empfangen, z.B. aus einem Online-Geschäft beziehen.

[0032] Die Identifikationsinformation wird von dem Nutzerendgerät **1**, **2** abgesichert an den Netzwerkteilnehmer **3** gesendet, beispielsweise signiert auf Basis einer Public-Key-Kryptographie, wie durch die oben beschriebene Initialisierungsphase ermöglicht. In diesem Beispiel kann das Nutzerendgerät **1**, **2** von dem Netzwerkteilnehmer **3** auf Anfrage eine Nonce erhalten, welche zur abgesicherten Übermittlung eingesetzt werden kann.

[0033] Zusammen mit der Übermittlung der Identifikationsinformation oder separat sendet das Nutzerendgerät **1**, **2** an den Netzwerkteilnehmer **3** in Schritt **204** eine Aufforderung, das Gerät **14** an das Netzwerk anzubinden.

[0034] Diese Aufforderung und die Identifikationsinformationen werden vorzugsweise verschlüsselt übertragen, schon um zu verhindern, dass sich ein Angreifer durch Ermittlung der Identifikationsinformation als anzubindendes Gerät **14** ausgeben kann. Die Verschlüsselung erfolgt dabei vorzugsweise auf Basis der in der Initialisierungsphase ausgetauschten Informationen. Insbesondere können die beiden Teilnehmer sich auf Basis der dabei ausgetauschten Zertifikate mit einem vorgegebenen Protokoll auf einen gemeinsamen Schlüssel einigen (Key agreement protocol). Hierzu bieten sich beispielsweise Diffie-Hellman-Verfahren oder RSA-Verfahren entsprechend der NIST Special Publication 800-56B an. Alternativ kann die Verschlüsselung auf Basis eines öffentlichen Verschlüsselungsverfahrens wie z.B. einem RSA-OAEP-Verfahren erfolgen.

[0035] Der Netzwerkteilnehmer **3** überprüft (z.B. anhand der beschriebenen Public-Key-Kryptographie), ob die Nachricht mit der Aufforderung bzw. der Identifikationsinformation von einer vertrauenswürdigen Quelle stammen. Werden die empfangene Aufforderung und die empfangene Identifikationsinformation als vertrauenswürdig bestätigt, kann zwischen dem Netzwerkteilnehmer **3** und dem anzubindenden Gerät **14** eine abgesicherte Kommunikationsverbindung aufgebaut werden, wie als Schritt **205** dargestellt. Hierzu kann insbesondere eine Schlüsselaushandlung zwischen dem Netzwerkteilnehmer **3** und dem anzubindenden Gerät **14** stattfinden, um einen gemeinsamen, geheimen Schlüssel zu etablieren, auf dessen Basis eine abgesicherte Kommunikation erfolgen kann. Die Einigung auf einen gemeinsamen, geheimen Schlüssel kann zum Beispiel auf Mechanismen der Public-Key-Kryptographie beruhen, z.B. dem Diffie-Hellman Schlüssel-Austausch-Protokoll. Vorzugsweise erfolgt aber ein Mechanismus basierend auf der sogenannten Physical Layer Security. Dabei werden Schlüssel für symmetrische Verfahren automatisch auf der Grundlage physikalischer Eigenschaften der Übertragungskanäle zwischen den involvierten Knoten erzeugt, wobei die Reziprozität und die inhärente Zufälligkeit dieser Übertragungskanäle ausgenutzt werden.

[0036] Wurde ein gemeinsamer, geheimer Schlüssel sowohl im Netzwerkteilnehmer **3** als auch im anzubindenden Gerät **14** etabliert, kann auf dessen Basis eine verschlüsselte Kommunikation zwischen den beiden erfolgen. Das Gerät **14** ist somit sicher an das Netzwerk angebunden. Während also eine abgesicherte Kommunikation zwischen dem Gerät **14** und dem Netzwerk nun erfolgen kann, ist eine gegenseitige Authentifizierung des Geräts **14** und des Netzwerkteilnehmers **3** bisher noch nicht sichergestellt. Dies erfolgt nun auf Basis der vom Nutzerendgerät an den Netzwerkteilnehmer übermittelten Identifikationsinformation in Schritt **206**.

[0037] In einem ersten Ausführungsbeispiel erzeugt das anzubindende Gerät **14** nach der erfolgreichen Schlüsselerzeugung eine Zufallszahl R1 und schickt diese an den Netzwerkteilnehmer **3**. Die Zufallszahl wird dabei mit dem gemeinsamen Schlüssel verschlüsselt. Der Netzwerkteilnehmer **3** entschlüsselt die Nachricht mit dem gemeinsamen Schlüssel und erhält somit die Zufallszahl R1. Der Netzwerkteilnehmer **3** erzeugt nun eine Zeichenkette auf Basis der Zufallszahl R1 und der Identifikationsinformation, z.B. fügt er die Zufallszahl und die Identifikationsinformation zusammen (Konkatenation). Der Netzwerkteilnehmer **3** berechnet nun vorzugsweise eine Abbildung über die Zeichenkette, z.B. über eine Streuwertfunktion bzw. Hashwertbildung. Zudem erzeugt er seinerseits eine Zufallszahl R2 und fügt diese der Zeichenkette der Abbildung hinzu und sendet die resultierende Nachricht (wiederum mit dem gemeinsamen Schlüssel verschlüsselt) an das zu authentifizierende Gerät **14**.

[0038] Um zu verhindern, dass ein Angreifer sich gegenüber dem zu authentifizierenden Gerät **14** als der Netzwerkteilnehmer **3** ausgeben kann, indem er aus der Nachricht die Identifikationsinformationen ableitet, sollte die Abbildung ein Einwegfunktion sein bzw. eine Preimage-Resistance aufweisen und die Identifikationsinformation eine ausreichende Länge haben.

[0039] Anstelle einer Streuwert- oder Hashwertfunktion kann die Abbildung auch auf einer anderen Funktion beruhen, welche auf Teile der Zufallszahl R1 und Teile der Identifikationsinformationen angewandt wird. Zum Beispiel könnte die Funktion in einer XOR-Verknüpfung einer n-Bit-Zufallszahl und der ersten Hälfte einer 2n-Bit-Identifikationsinformation bestehen.

[0040] Das zu authentifizierende Gerät **14** empfängt die Nachricht von dem Netzwerkteilnehmer **3**, entschlüsselt diese mit dem gemeinsamen Schlüssel und erhält somit die Zufallszahl R2 sowie die Abbildung der Zeichenkette aus Zufallszahl R1 und Identifikationsinformation. Da das zu authentifizierende Gerät **14** seine eigene Identifikationsinformation und auch die Zufallszahl R1 kennt, kann es die Abbildung (mit der gleichen Abbildungsfunktion wie der Netzwerkteilnehmer) selbst berechnen und mit der empfangenen Abbildung vergleichen. Bei Übereinstimmung wird die Nachricht des Netzwerkteilnehmers **3** als Antwort auf die Zufallszahl R1 als vertrauenswürdig eingestuft und somit der Netzwerkteilnehmer **3** durch das Gerät **14** authentifiziert.

[0041] Im nächsten Schritt berechnet das zu authentifizierende Gerät **14** analog zum oben beschriebenen Vorgang auf Basis der empfangenen Zufallszahl R2 und der Identifikationsinformation eine weitere Abbildung. Dieser Abbildung hängt das Gerät **14** optionalerweise die Zufallszahl R1 an und schickt die resultierende Nachricht mit dem gemeinsamen Schlüssel verschlüsselt an den Netzwerkteilnehmer **3**. Der Netzwerkteilnehmer **3** entschlüsselt die Nachricht mit dem gemeinsamen Schlüssel und erhält somit die weitere Abbildung (und gegebenenfalls wiederum die Zufallszahl R1). Da der Netzwerkteilnehmer **3** die Identifikationsinformation und die Zufallszahl R2 kennt, kann er durch Berechnung einer entsprechenden Abbildung die weitere Abbildung verifizieren. Stimmen die beiden Abbildungen überein, wird die Nachricht des zu authentisierenden Geräts **14** als vertrauenswürdig eingestuft und das Gerät **14** von dem Netzwerkteilnehmer **3** authentifiziert.

[0042] Optionalerweise kann nun der Netzwerkteilnehmer **3** noch eine Nachricht an das Nutzerendgerät **1**, **2** senden und diesem die erfolgreiche Anbindung und Authentifizierung des Geräts **14** mitteilen.

[0043] Eine Hauptanwendung für Verfahren wie die beschriebenen ist die Heimautomatisierung (Smart Home). In einem solchen Szenario besteht jedes individuelle Netzwerk gewöhnlicherweise aus einer verhältnismäßig niedrigen Zahl an Knoten (z.B. 10 bis 30), die Knoten bleiben für einen relativ langen Zeitraum an das Netzwerk angebunden (z.B. mehrere Monate bis mehrere Jahre) und es ist sehr schwer für einen Angreifer festzustellen, wann und wie der Endverbraucher neue Knoten kaufen und an das Netzwerk anbinden will. Unter solchen Umständen kann angenommen werden, dass die Kenntnis von Identifikationsinformationen über einen Knoten den rechtmäßigen Besitzer des Knotens anzeigt. Die gegenseitige Authentifizierung baut auf dieser Annahme auf, indem sie verlangt, dass die kommunizierenden Parteien, also das anzubindende Gerät und der Netzwerkteilnehmer, sich gegenseitige nachweisen, dass sie beide Kenntnis der Identifikationsinformationen über den anzubindenden Knoten besitzen. In einem solchen Szenario ist auch der Einsatz eines mit dem Netzwerk verknüpften Nutzerendgerät sinnvoll. Da das Nutzerendgerät im Gegensatz zu den gewöhnlichen Sensor- oder Aktor-Knoten eines Heimnetzwerks über eine Nutzerschnittstelle und Rechenkapazitäten verfügt, kann dieses auf andere Weise sicher mit dem Netzwerk verbunden werden und das Verfahren zur Anbindung von Sensor- und Aktor-Knoten auf dieser Basis erfolgen.

[0044] Ein zweites Ausführungsbeispiel für die Anbindung neuer Knoten **14** an ein bestehendes Netzwerk (beispielsweis in Sterntopologie) geht davon aus, dass das anzubindende Gerät **14** zweite Identifikationsinformationen besitzt, und zwar Identifikationsinformationen über den Netzwerkteilnehmer **3**. Diese können zum Beispiel über das Nutzerendgerät **1**, **2** auf das Gerät **14** übertragen worden sein. Wie im vorangegangenen Beispiel wird von einer sicheren Kommunikation zwischen Nutzerendgerät **1**, **2** und Netzwerkteilnehmer **3** ausgegangen, die ersten Identifikationsinformationen werden von dem Nutzerendgerät **1**, **2** an den Netzwerkteilnehmer **3** übertragen, auf eine Aufforderung des Nutzerendgerätes **1**, **2** hin starten Netzwerkteilnehmer **3** und anzubindendes Gerät **14** eine Schlüsselaushandlung, der Netzwerkteilnehmer **3** sendet dem Gerät **14** eine Nachricht auf Basis einer Zufallszahl und der ersten Identifikationsinformation und das Gerät **14** authentifiziert den Netzwerkteilnehmer **3** auf Basis dieser Nachricht. Soweit entspricht das alternative Protokoll den zu **Fig.** 2 beschriebenen Schritten **201** bis **205** sowie der ersten Nachricht des Schritts **206** im ersten Ausführungsbeispiel.

[0045] Im nächsten Schritt dieses zweiten Ausführungsbeispiels sendet das Gerät **14** wiederum an den Netzwerkteilnehmer **3** eine Nachricht auf Basis der Zufallszahl R2 des Netzwerkteilnehmers **3** und einer Identifikationsinformation, in dieser Ausführung allerdings der zweiten Identifikationsinformation, also der Identifikationsinformation über den Netzwerkteilnehmer **3**. Der Netzwerkteilnehmer **3** entschlüsselt wiederum die Nachricht und vergleicht die darin enthaltenen Informationen auf Basis der Zufallszahl R2 und der zweiten Identifikationsinformation mit den entsprechenden gespeicherten Werten, über die er verfügt.

[0046] Im Unterschied zum ersten Ausführungsbeispiel ist es in diesem Ausführungsbeispiel eher möglich, auf eine Abbildungsfunktion über die Zufallszahlen und Identifikationsinformationen zu verzichten. Sowohl die Nachricht mit der Zufallszahl R1 und der ersten Identifikationsinformation als auch die Nachricht mit der Zufallszahl R2 und der zweiten Identifikationsinformation können (mit gewissen Sicherheitseinbußen) ohne Abbildungsfunktion, also lediglich mit dem gemeinsamen Schlüssel verschlüsselt übertragen werden, da auf zwei verschiedene Identifikationsinformationen zurück gegriffen wird. Allerdings müssen diese Informationen auch in den beiden Verfahrensteilnehmern vorhanden sein, was einen etwas größeren Aufwand für Informationsmanagement mit sich bringt.

[0047] In einem dritten Ausführungsbeispiel für die gegenseitige Authentifizierung eines Netzwerkteilnehmers **3** und eines anzubindenden Geräts **14** und für die Anbindung des Geräts **14** an das Netzwerk wird wiederum eine verschlüsselte Verbindung zwischen Netzwerkteilnehmer **3** und anzubindendem Gerät **14** auf Aufforderung eines Nutzerendgeräts **1**, **2** hergestellt. Zusätzlich zu dieser Sicherheit der Übertragung wird die Authentizität des Netzwerkteilnehmers **3** und des Geräts **14** wiederum auf Basis der Identifikationsinformation sicher gestellt. Hierzu wird ein Nachrichtenauthentifizierungscode (message authentification code, MAC) auf Basis der Identifikationsinformation (über das Gerät **14**) verwendet.

[0048] Wie in den vorigen Beispielen kennen wiederum das anzubindende Gerät **14** und der Netzwerkteilnehmer **3** die Identifikationsinformation über das Gerät **14**, diese stellt somit ein geteiltes Geheimnis zwischen ihnen dar. Sowohl der Netzwerkteilnehmer als auch das Gerät berechnen nun auf Basis dieses gemeinsamen Geheimnisses den gleichen Nachrichtenauthentifizierungscode. Dieser Nachrichtenauthentifizierungscode kann mit dem gemeinsamen Schlüssel für die verschlüsselte Kommunikation verknüpft werden.

[0049] In einer vorteilhaften Variante des Ausführungsbeispiels werden auf Basis des geheimen Schlüssels und der Identifikationsinformation mittels MAC-Mechanismen zwei Schlüssel für die weitere Kommunikation zwischen dem Netzwerkteilnehmer und dem Gerät erzeugt, einer für die Verschlüsselung, einer für die Authentifizierung. Alternativ kann lediglich ein Schlüssel abgeleitet werden dieser als Ausgangsbasis für ein authentifiziertes Verschlüsselungsschema verwendet werden.

[0050] Mit einem Verfahren nach diesem Ausführungsbeispiel kann ein Angreifer die verwendeten Geheimnisse ohne vorherige Kenntnis nicht aus der Kommunikation ableiten, da alle verwendeten Funktionen Einwegfunktionen sind. Vorteilhafterweise wird als Nachrichtenauthentifizierungscode HMAC verwendet, aber auch Nachrichtenauthentifizierungscodes auf der Basis von Pseudo-Zufallsfunktionen, wie beispielsweise CMAC, können eingesetzt werden.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- DE 102009002396 A1 [0009]
- DE 102009045133 A1 [0009]

Zitierte Nicht-Patentliteratur

- B. Clifford Neuman and Theodore Ts'o: "Kerberos: An Authentication Service for Computer Networks", IEEE Communications 32 (9) : 33–8. doi:10.1109/35.312841, September 1994 [0010]
- NIST Special Publication 800-56B [0034]

Patentansprüche

1. Verfahren zur gegenseitigen Authentifizierung eines Geräts und eines Teilnehmers eines Netzwerks und zur Anbindung des Geräts an das Netzwerk durch den Teilnehmer, **dadurch gekennzeichnet,** dass der Teilnehmer von einem Nutzerendgerät eine erste Identifikationsinformation über das anzubindende Gerät sowie eine Aufforderung empfängt, das Gerät an das Netzwerk anzubinden, dass der Teilnehmer das Gerät an das Netzwerk anbindet, indem es eine verschlüsselte Kommunikationsverbindung mit ihm aufbaut, und dass das Gerät und der Teilnehmer sich über die verschlüsselte Kommunikationsverbindung unter Verwendung der ersten Identifikationsinformation gegenseitig authentifizieren.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,** dass das Nutzerendgerät und der Teilnehmer über eine abgesicherte Kommunikationsverbindung verfügen.

3. Verfahren nach einem der vorangegangenen Ansprüche, **dadurch gekennzeichnet,** dass das Nutzerendgerät und der Teilnehmer sich vor der Authentifizierung des Geräts und des Teilnehmers und der Anbindung des Geräts gegenseitig authentifizieren.

4. Verfahren nach einem der vorangegangenen Ansprüche, **dadurch gekennzeichnet,** dass die gegenseitige Authentifizierung von Gerät und Teilnehmer auf Basis einer Verknüpfung der ersten Identifikationsinformation mit Zufallszahlen erfolgt.

5. Verfahren nach einem der vorangegangenen Ansprüche, **dadurch gekennzeichnet,** dass zur gegenseitigen Authentifizierung das Gerät in einer ersten Nachricht eine erste Zufallszahl verschlüsselt an den Teilnehmer sendet, der Teilnehmer eine zweite Nachricht auf Basis der ersten Identifikationsinformation, der ersten Zufallszahl und einer zweiten Zufallszahl verschlüsselt an das Gerät sendet, das Gerät die zweite Nachricht entschlüsselt und den Teilnehmer auf Basis der entschlüsselten zweiten Nachricht authentifiziert, das Gerät eine dritte Nachricht auf Basis der ersten Identifikationsinformation und der zweiten Zufallszahl verschlüsselt an den Teilnehmer sendet und der Teilnehmer die dritte Nachricht entschlüsselt und das Gerät auf Basis der entschlüsselten dritten Nachricht authentifiziert.

6. Verfahren nach Anspruch 4, **dadurch gekennzeichnet,** dass zur gegenseitigen Authentifizierung der Teilnehmer in einer ersten Nachricht eine erste Zufallszahl verschlüsselt an Gerät sendet, das Gerät eine zweite Nachricht auf Basis der ersten Identifikationsinformation, der ersten Zufallszahl und einer zweiten Zufallszahl verschlüsselt an den Teilnehmer sendet, der Teilnehmer die zweite Nachricht entschlüsselt und das Gerät auf Basis der entschlüsselten zweiten Nachricht authentifiziert, der Teilnehmer eine dritte Nachricht auf Basis der ersten Identifikationsinformation und der zweiten Zufallszahl verschlüsselt an das Gerät sendet sowie das Gerät die dritte Nachricht entschlüsselt und den Teilnehmer auf Basis der entschlüsselten dritten Nachricht authentifiziert.

7. Verfahren nach einem der Anspruch 5 oder 6, **dadurch gekennzeichnet,** dass die zweite Nachricht verschlüsselt eine erste Abbildung der ersten Zufallszahl und der ersten Identifikationsinformation, insbesondere das Ergebnis einer Streuwertfunktion, welche auf die Konkatenation der ersten Zufallszahl und der ersten Identifikationsinformation angewandt wurde, sowie die zweite Zufallszahl enthält und die dritte Nachricht verschlüsselt eine zweite Abbildung der zweiten Zufallszahl und der ersten Identifikationsinformation, insbesondere das Ergebnis einer Streuwertfunktion, welche auf die Konkatenation der zweiten Zufallszahl und der ersten Identifikationsinformation angewandt wurde, enthält.

8. Verfahren nach Anspruch 7, **dadurch gekennzeichnet,** dass die Authentifizierungen durch das Gerät und den Teilnehmer jeweils durch Vergleich der empfangenen und entschlüsselten Abbildungen mit einer entsprechend durch das Gerät und den Teilnehmer selbst gebildeten Abbildung erfolgt.

9. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet,** dass zur gegenseitigen Authentifizierung das Gerät in einer ersten Nachricht eine erste Zufallszahl verschlüsselt an den Teilnehmer sendet, der Teilnehmer eine zweite Nachricht auf Basis der ersten Identifikationsinformation, der ersten Zufallszahl und einer zweiten Zufallszahl verschlüsselt an das Gerät sendet, das Gerät die zweite Nachricht entschlüsselt und den Teilnehmer auf Basis der entschlüsselten zweiten Nachricht authentifiziert, das Gerät eine dritte Nachricht auf Basis einer zweiten Identifikationsinformation über den Teilnehmer und der zweiten Zufallszahl verschlüsselt an den Teilnehmer sendet und der Teilnehmer die dritte Nachricht entschlüsselt und das Gerät auf Basis der entschlüsselten dritten Nachricht authentifiziert.

10. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet,** dass die gegenseitige Authentifizierung erfolgt, indem das Gerät und der Teilnehmer über einen Nachrichtenauthentifizierungscode auf Basis der ersten Identifikationsinformation, insbesondere auf Basis einer Verknüpfung der ersten Identifikationsinformation mit einem Schlüssel der verschlüsselten Kommunikationsverbindung, kommunizieren.

11. Teilnehmer an einem Netzwerk der eingerichtet ist, von einem Nutzerendgerät eine erste Identifikati-

onsinformation über ein anzubindendes Gerät sowie eine Aufforderung zur Anbindung des Geräts an das Netzwerk zu empfangen, das Gerät an das Netzwerk anzubinden, indem es eine verschlüsselte Kommunikationsverbindung mit ihm aufbaut, sich gegenüber dem Gerät über die verschlüsselte Kommunikationsverbindung unter Verwendung der ersten Identifikationsinformation zu authentisieren und das Gerät über die verschlüsselte Kommunikationsverbindung unter Verwendung der ersten Identifikationsinformation zu authentifizieren.

12. Computerprogramm, welches eingerichtet ist, alle Schritte eines Verfahrens gemäß einem der Ansprüche 1 bis 10 durchzuführen.

13. Maschinenlesbares Speichermedium, auf welchem ein Computerprogramm nach Anspruch 12 gespeichert ist.

Es folgen 2 Seiten Zeichnungen

Anhängende Zeichnungen

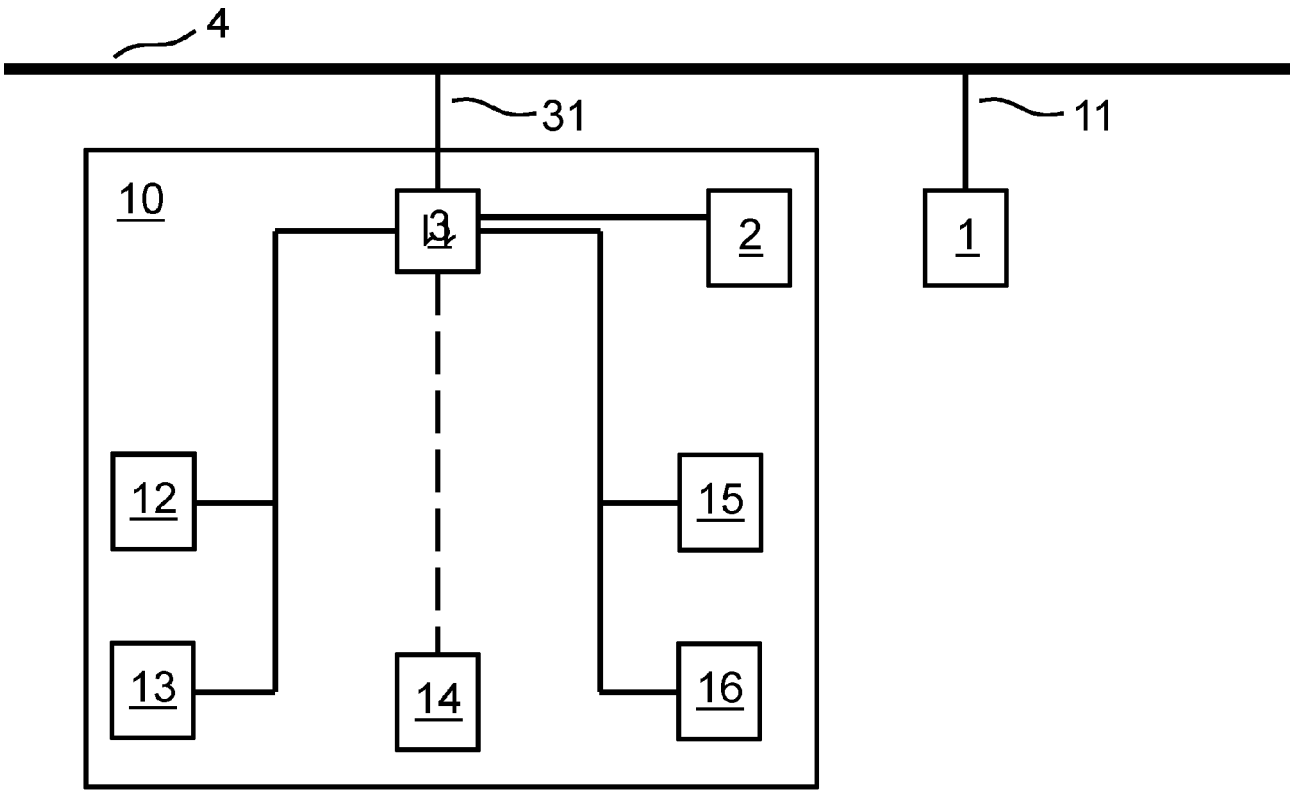


Fig. 1

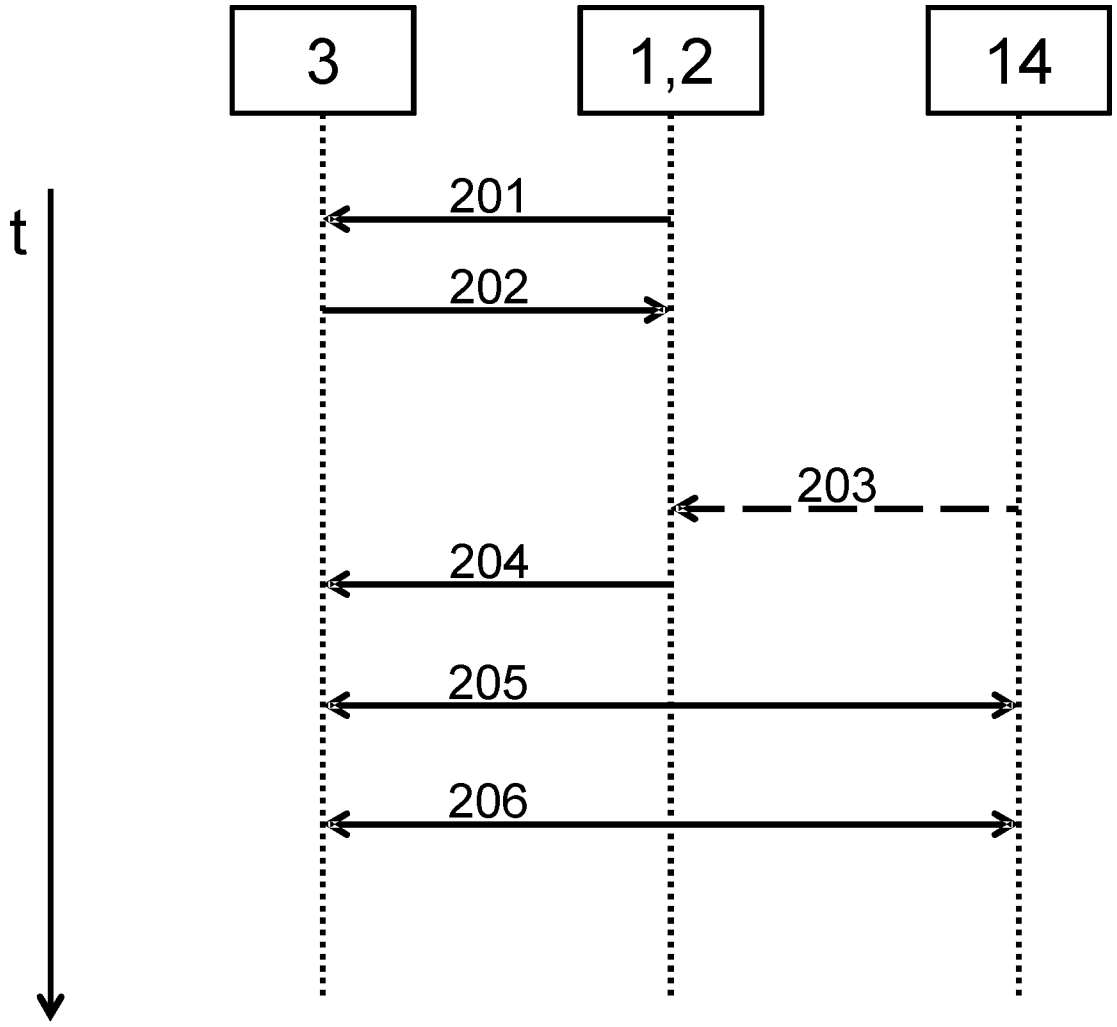


Fig. 2