(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 10 2008 046 563 A1** 2010.03.11

(12) **Offenlegungsschrift**

(21) Aktenzeichen: **10 2008 046 563.1**
(22) Anmeldetag: **10.09.2008**
(43) Offenlegungstag: **11.03.2010**

(51) Int Cl.[8]: ***H04L 9/28*** (2006.01)

(71) Anmelder:
Siemens Aktiengesellschaft, 80333 München, DE

(72) Erfinder:
Falk, Rainer, Dr., 85435 Erding, DE; Hof, Hans-Joachim, Dr., 80337 München, DE; Meyer, Ulrike, Dr., 80469 München, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

US 2005/00 50 004 A1

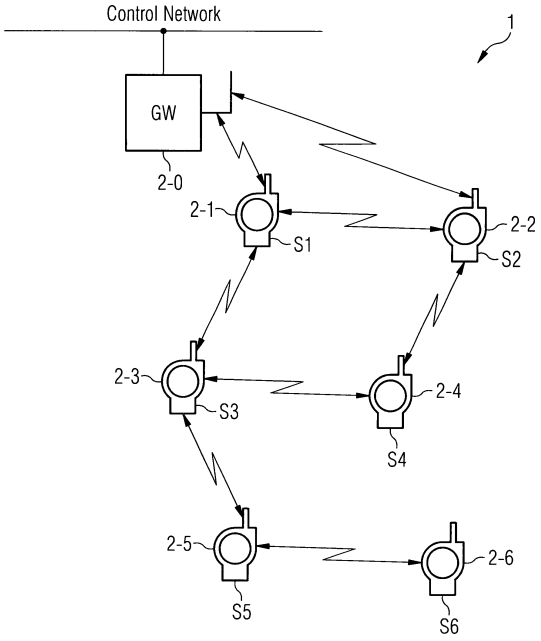
IEEE Std 802.15.4-2006: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs). 8. September 2006, S. 13, 138, 197-215

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gemäß § 44 PatG ist gestellt.

(54) Bezeichnung: **Verfahren zur Datenübertragung zwischen Netzwerkknoten**

(57) Zusammenfassung: Die Erfindung schafft ein Verfahren zur kryptographisch geschützten Übertragung von Daten zwischen Netzwerkknoten (2) eines Netzwerkes (1). Die Netzwerkknoten (2) sind beispielsweise Sensorknoten eines drahtlosen Sensornetzwerkes. Bei dem erfindungsgemäßen Verfahren wird zur Übertragung der Daten in einer Nachricht (F) ein NONCE-Wert (N) aus einem Zählwert (CTR), welcher bei der Übertragung der Nachricht (F) aktualisiert wird, und aus einem Konstantwert (EANCV), welcher den Netzwerkknoten (2) des Netzwerkes (1) gemeinsam zur Verfügung gestellt wird, gebildet. Die Verschlüsselung und Entschlüsselung der in der Nachricht (F) übertragenen Daten innerhalb der Netzwerkknoten (2) erfolgt dann mittels eines kryptographischen Schlüssels (K) und des gebildeten NONCE-Wertes (N). Das erfindungsgemäße Verfahren bietet insbesondere Schutz gegen Replay-Attacken bei gleichzeitig minimalem Ressourcenaufwand der Netzwerkknoten (2).



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur kryptographisch geschützten Übertragung von Daten zwischen Netzwerkknoten eines Netzwerkes, insbesondere eines drahtlosen Sensornetzwerkes.

[0002] Drahtlose Sensornetzwerke oder Sensoraktornetze WSN (Wireless Sensor Networks) sind vielseitig einsetzbar. Beispielsweise werden drahtlose Sensornetzwerke zur Überwachung und Steuerung von Fertigungsanlagen, zur Überwachung und Steuerung von chemischen Prozessen sowie zur Überwachung von Pipelines eingesetzt. In drahtlosen Sensornetzen kommunizieren die Sensorknoten des Netzwerkes drahtlos über eine Funkschnittstelle. Die Datenübertragung erfolgt gemäß einem Datenübertragungsprotokoll. Bekannte Datenübertragungsprotokolle zur Datenübertragung über eine Funkschnittstelle sind das Protokoll 802.15.4, Zig Bee, Wireless HART sowie Bluetooth. Mittels Nachrichten werden zwischen den Sensorknoten Messwerte und Steuerkommandos ausgetauscht.

[0003] Um eine Manipulation der drahtlos übertragenen Nachrichten durch unbefugte Dritte zu verhindern, werden die zwischen den Knoten des Netzwerks ausgetauschten Daten kryptographisch geschützt. Aufgrund der eingeschränkten Leistungsfähigkeit von Netzwerkknoten, insbesondere in drahtlosen Sensornetzwerken, hinsichtlich Speicherplatz und Rechenleistung und aufgrund der begrenzten Energieressourcen, insbesondere bei einem Batteriebetrieb der Knoten, besteht daher ein Bedarf nach einer effizienten Sicherheitslösung.

[0004] Zur Sicherung der übertragenen Daten werden diese herkömmlicherweise mit einem Schlüssel verschlüsselt. Allerdings ist die einfache Verschlüsselung K nicht ganz sicher, da für einen Dritten die Möglichkeit besteht, Nachrichten in sogenannten ”Replay-Attacken” wiedereinzuspiegeln. Es werden daher in konventionellen Netzwerken sogenannte NONCE-Werte eingesetzt.

[0005] Ein NONCE-Wert stellt einen Einmal-Wert bzw. einen nur einmalig zu verwendenden Wert dar. Der NONCE-Wert dient zur Erkennung von wieder eingespielten Nachrichten (Replay-Attacken). Die Verschlüsselung der Daten, beispielsweise von Messdaten seitens eines Sendeknotens, beispielsweise eines Sensorknotens, erfolgt dann in Abhängigkeit von einem Schlüssel K und einem NONCE-Wert. Dieser NONCE-Wert wird auch als Initialisierungsvektor bezeichnet. Der Sendeknoten sendet eine Nachricht bzw. einen Frame F an einen Empfangsknoten innerhalb des Netzwerkes. Jeder NONCE-Wert wird in Verbindung mit jedem Schlüssel nur einmal verwendet. Um einen wirksamen Schutz gegen Wiedereinspielen von Nachrichten bzw. Replay-Attacken zu erreichen wird daher auf Seiten des Empfangsknotens die Einmaligkeit des in der empfangenen Nachricht verwendeten NONCE-Wertes überprüft. Oft verwendete kryptographische Verfahren zum Schutz von Datenframes, z. B. bei 802.15.4 oder WLAN, erfordern weiterhin, dass ein NONCE-Wert bzw. ein Initialisierungsvektor mit jedem Schlüssel nur einmal verwendet werden darf. Ansonsten würde der kryptographischen Schutz geschwächt werden. Spätestens wenn der Wertebereich für NONCE-Werte erschöpft ist, muss daher ein neuer Schlüssel K' eingerichtet werden (Re-Keying).

[0006] Bei einer Verwendung von NONCE-Werten zum Schutz gegen Replay-Attacken ist es allerdings notwendig, dass auf der Empfängerseite, das heißt auf Seiten eines Empfangsknotens Zustandsinformationen über bereits verwendete NONCE-Werte gespeichert werden. Da ein Netzwerk aus einer Vielzahl von Knoten bestehen kann und jeder Knoten für jeden anderen Knoten des Netzwerkes, von dem er potenziell eine Nachricht bzw. ein Frame empfangen kann, eine zugehörige Zustandsinformation über die von den jeweiligen Knoten bereits verwendeten NONCE-Werte speichern muss, führt dies zu einer hohen Ressourcenbelastung aufgrund des benötigten Speicherplatzes zum Abspeichern der Zustandsinformationen. Ein hoher Speicherbedarf in jedem Knoten besteht insbesondere dann, wenn viele Ende-zu-Ende-Sicherheitsbeziehungen zwischen den verschiedenen Knoten des Netzwerkes bestehen und da für jede Ende-zu-Ende-Sicherheitsbeziehung in dem Knoten ein NONCE-Wert gespeichert werden muss.

[0007] Es ist daher eine Aufgabe der vorliegenden Erfindung ein Verfahren zur kryptographisch geschützten Übertragung von Daten zwischen Netzwerkknoten eines Netzwerks zu schaffen, bei dem der benötigte Speicherplatz zum Speichern von Zustandsinformationen für NONCE-Werte gering ist.

[0008] Diese Aufgabe wird durch ein Verfahren zum kryptographisch geschützten Übertragen von Daten zwischen Netzwerkknoten eines Netzwerkes mit den im Patentanspruch 1 angegebenen Merkmalen gelöst.

[0009] Die Erfindung schafft ein Verfahren zum kryptographisch geschützten Übertragen von Daten zwischen Netzwerkknoten eines Netzwerks, wobei zur Übertragung der Daten in einer Nachricht die folgenden Schritte ausgeführt werden:

a) Bilden eines NONCE-Wertes, aus einem Zählwert, welcher bei der Übertragung der Nachricht aktualisiert wird, und aus einem Konstantwert, welcher den Netzwerkknoten des Netzwerkes gemeinsam zur Verfügung gestellt wird; und

b) Ver- und Entschlüsseln der in der Nachricht übertragenen Daten mittels eines kryptographi-

schen Schlüssels und des gebildeten NONCE-Wertes.

[0010] Bei einer Ausführungsform des erfindungsgemäßen Verfahrens wird der gemeinsame, netzwerkweit eingesetzte Konstantwert von einem zentralen Management-Netzwerkknoten den übrigen Netzwerkknoten des Netzwerks bereitgestellt.

[0011] Dies bietet den Vorteil, dass der netzwerkweit eingesetzte Konstantwert in einfacher Weise verwaltet und gegebenenfalls ohne großen Aufwand ausgetauscht werden kann, um die Sicherheit des Netzwerks gegen Manipulationen zu erhöhen. Der netzwerkweit eingesetzte Konstantwert muss auf einem Netwerkknoten nur einmal gespeichert werden unabhängig von der Anzahl der Netzwerkknoten. Weiterhin ist es nicht erforderlich, dass ein Netzwerkknoten einen Zählerwert dauerhaft speichert, also auch z. B. bei Abklemmen der Stromversorgung oder bei einem Batteriewechsel, um zu verhindern, dass der gleiche Nonce-Wert durch diesen Netzwerkknoten mehrmals verwendet wird, da nach Anlegen der Stromversorgung an den Netzwerkknoten und Aufnahme des Betriebs ihm ein aktueller netzwerkweit eingesetzte Konstantwert zugewiesen werden kann.

[0012] Bei einer Ausführungsform des erfindungsgemäßen Verfahrens wird der NONCE-Wert zusätzlich in Abhängigkeit von einer Sendeknotenadresse desjenigen Sendenetzwerkknotens gebildet, der die Nachricht zu einem Empfangsnetzwerkknoten des Netzwerks überträgt.

[0013] Hierdurch wird die Sicherheit gegenüber Replay-Attacken weiter gesteigert.

[0014] Bei einer Ausführungsform des erfindungsgemäßen Verfahrens wird der gemeinsame Konstantwert von dem zentralen Management-Netzwerkknoten durch Aussenden einer Broadcast-Nachricht oder durch Aussenden von Unicast-Nachrichten an die Netzwerkknoten des Netzwerks übertragen.

[0015] Dadurch kann der gemeinsame, netzwerkweit eingesetzte Konstantwert in einfacher und schneller Weise aktualisiert werden.

[0016] Bei einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens ist der gemeinsame Konstantwert von dem zentralen Management-Netzwerkknoten umkonfigurierbar.

[0017] Diese Umkonfiguration des gemeinsamen Konstantwertes erfolgt bei einer möglichen Ausführungsform in festen, regelmäßigen Zeitabständen.

[0018] Bei einer alternativen Ausführungsform erfolgt die Umkonfiguration des gemeinsamen Konstantwertes, der zur Bildung eines NONCE-Wetes verwendet wird, nach Überschreiten einer vorgegebenen übertragenen Datenmenge.

[0019] Bei einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens erfolgt die Umkonfiguration des gemeinsamen Konstantwertes nach einem Überschreiten einer vorgegebenen Anzahl von übertragenen Nachrichten.

[0020] Bei einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens erfolgt die Umkonfiguration des gemeinsamen Konstantwertes nach Erreichen eines vorgegebenen Zählerwertes bei einem der Netzwerkknoten des Netzwerkes.

[0021] Bei einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens erfolgt die Umkonfiguration des gemeinsamen Konstantwertes bei Eintritt eines vorgegebenen Ereignisses.

[0022] Bei einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens ist das vorgegebene Ereignis die Aufnahme eines zusätzlichen Netzwerkknotens in das Netzwerk, beispielsweise wenn sich ein Netzwerkknoten nach Anschließen einer Versorgungsspannung eine Kommunikation mit dem Netzwerk aufnimmt.

[0023] Bei einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens erfolgt die Umkonfiguration des gemeinsamen Konstantwertes bei einer Übertragung von Daten, die eine vorgegebene Bedingung erfüllen.

[0024] Die verschiedenen Ausführungsformen zur Umkonfiguration des gemeinsamen Konstantwertes erlauben es das erfindungsgemäße Verfahren zur kryptographisch geschützten Übertragung von Daten zwischen Netzwerkknoten eines Netzwerks für die verschiedensten Anwendungen flexibel einzusetzen und den verschiedenen Sicherheitsbedürfnissen zu genügen.

[0025] Bei einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens wird der NONCE-Wert durch Konkatenation bzw. Verkettung der Sendeknotenadresse des sendenden Netzwerkknotens, des gemeinsamen Konstantwertes und eines Zählwertes, der von einem internen Zähler des sendenden Netzwerkknotens erzeugt wird, gebildet.

[0026] Diese Ausführungsform bietet den Vorteil, dass der NONCE-Wert mit einem relativ geringen schaltungstechnischen Aufwand bei gleichzeitig geringem Strom bzw. Energieverbrauch gebildet werden kann.

[0027] Bei einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens wird der NONCE-Wert durch eine Hash-Funktion der Konkatenation der

Sendeknotenadresse des sendenden Netzwerkknotens, des gemeinsamen Konstantwerts und des Zählwertes, der von einem internen Zählers des sendenden Netzwerkknotens erzeugt wird, gebildet.

[0028] Diese Ausführungsform bildet den Vorteil, dass ein Dritter, selbst beim Abhören einer übertragenen Nachricht nicht den von dem Sendenetzwerkknoten aktuell verwendeten NONCE-Wert erkennen kann, so dass die Sicherheit gegenüber Manipulationen erhöht wird.

[0029] Bei einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens erfolgt das Verschlüsseln und Entschlüsseln der in der Nachricht übertragenen Daten durch einen CCM-Algorithmus.

[0030] Bei einer möglichen Ausführungsform des Verfahrens weist die übertragenen Nachricht Header-Daten auf, welche eine Sendeknotenadresse, eine Empfangsknotenadresse und den aktuellen Zählwert des Sendenetzwerkknotens umfassen, sowie Nutzdaten, welche die verschlüsselten Daten enthalten.

[0031] Bei einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens vergleicht der Empfangsnetzwerkknoten den in der Nachricht übertragenen Zählwert des Sendenetzwerkknotens mit einem anhand der in der Nachricht übertragenen Sendeknotenadresse selektierten Zählwert eines internen Zählers des Empfangsnetzwerkknotens und bildet aus dem übertragenen Zählwert, aus dem gemeinsamen Konstantwert und aus der übertragenen Sendeknotenadresse einen empfangsseitigen NONCE-Wert, falls der übertragene Zählwert aktueller ist als der selektierte Zählwert, wobei der empfangsseitig gebildete NONCE-Wert und ein in dem Empfangsnetzwerkknoten gespeicherter Schlüssel zur Entschlüsselung der in der Nachricht verschlüsselt übertragenen Daten benutzt werden.

[0032] Bei einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens wird die Nachricht über eine Funkschnittstelle von dem Sendenetzwerkknoten zu dem Empfangsnetzwerkknoten übertragen.

[0033] Die Erfindung schafft ferner ein Netzwerk, bestehend aus mehreren Netzwerkknoten, die untereinander Daten in Nachrichten übertragen, wobei jeder Netzwerkknoten aufweist:

a) eine Einheit zum Bilden eines NONCE-Wertes, aus einem Zählwert, welcher bei der Übertragung einer Nachricht aktualisiert wird, und aus einem Konstantwert, welcher den Netzwerkknoten des Netzwerkes gemeinsam zur Verfügung gestellt wird; und

b) eine Einheit zur Ver- und Entschlüsselung der in der Nachricht übertragenen Daten mittels eines kryptographischen Schlüssels und des gebildeten NONCE-Wertes.

[0034] Bei einer Ausführungsform des erfindungsgemäßen Netzwerks weist das Netzwerk einen zentralen Management-Netzwerkknoten auf, der den gemeinsamen Konstantwert den übrigen Netzwerkknoten des Netzwerks zur Verfügung stellt.

[0035] Bei einer Ausführungsform des erfindungsgemäßen Netzwerks weist jeder Netzwerkknoten jeweils mindestens einen Sensor auf.

[0036] Die Erfindung schafft ferner ein Computerprogramm mit Programmbefehlen zur Durchführung eines Verfahrens zum kryptographisch geschützten Übertragen von Daten zwischen Netzwerkknoten eines Netzwerks, wobei zur Übertragung der Daten in eine Nachricht die folgenden Schritte ausgeführt werden:

a) Bilden eines NONCE-Wertes, aus einem Zählwert, welcher bei der Übertragung der Nachricht aktualisiert wird, und aus einem Konstantwert, welcher den Netzwerkknoten des Netzwerkes gemeinsam zur Verfügung gestellt wird; und

b) Ver- und Entschlüsseln der in der Nachricht übertragenen Daten mittels eines kryptographischen Schlüssels und des gebildeten NONCE-Wertes.

[0037] Die Erfindung schafft ferner einen Datenträger, der ein derartiges Computerprogramm speichert.

[0038] Im Weiteren werden bevorzugte Ausführungsformen des erfindungsgemäßen Verfahrens zur kryptographisch geschützten Übertragung von Daten zwischen Netzwerkknoten eines Netzwerks und des erfindungsgemäßen Netzwerkes unter Bezugnahme auf die beigefügten Figuren zur Erläuterung erfindungswesentlicher Merkmale beschrieben.

[0039] Es zeigen:

[0040] Fig. 1 ein einfaches Ablaufdiagramm zur Darstellung eines Ausführungsbeispiels des erfindungsgemäßen Verfahrens zum kryptographisch geschützten Übertragen von Daten;

[0041] Fig. 2 ein einfaches Blockdiagramm zur Darstellung der Übertragung einer Nachricht zwischen einem Sendeknoten und einem Empfangsknoten des erfindungsgemäßen Netzwerks;

[0042] Fig. 3 ein Diagramm zur Darstellung eines möglichen Datenformates einer bei dem erfindungsgemäßen Verfahren übertragenen Nachricht;

[0043] Fig. 4 ein Blockdiagramm eines Ausführungsbeispiels eines in dem erfindungsgemäßen Netzwerk enthaltenen Netzwerkknotens zur Darstel-

lung einer Verschlüsselung von Daten;

[0044] Fig. 5 ein Blockdiagramm eines Ausführungsbeispiels eines in dem erfindungsgemäßen Netwerk enthaltenen Empfangsknotens zur Darstellung der Entschlüsselung einer Nachricht;

[0045] Fig. 6 ein Beispiel für ein erfindungsgemäßes Netzwerk bei dem Nachrichten zwischen Netzwerkknoten nach dem erfindungsgemäßen Verfahren übertragen werden;

[0046] Fig. 7A, Fig. 7B verschiedene Varianten zur Bereitstellung eines gemeinsamen Konstantwerts durch einen zentralen Management-Netzwerkknotens bei dem erfindungsgemäße Verfahren;

[0047] Fig. 8 ein Ausführungsbeispiel eines erfindungsgemäßen Netzwerks;

[0048] Fig. 9 ein weiteres Ausführungsbeispiel eines erfindungsgemäßen Netwerks;

[0049] Fig. 10 ein weiteres Ausführungsbeispiel eines erfindungsgemäßen Netzwerks.

[0050] Wie man aus Fig. 1 erkennen kann, umfasst das erfindungsgemäße Verfahren zum kryptographisch geschützten Übertragen von Daten zwischen Netzwerkknoten eines Netzwerks im Wesentlichen zwei Schritte.

[0051] In einem ersten Schritt S1 wird ein NONCE-Wert N gebildet. Dieser NONCE-Wert N wird von einem Zählwert CTR, welcher bei der anschließenden Übertragung der Nachricht bzw. des Frames F aktualisiert wird und aus einem Konstantwert EANCV (Externally Assigned Nonce Contribution Value) gebildet. Dieser netzwerkweit eingesetzte gemeinsame Konstantwert EANCV wird den Netzwerkknoten des erfindungsgemäßen Netzwerks gemeinsam zur Verfügung gestellt. Bei einer möglichen Ausführungsform wird der netzwerkweit eingesetzte Konstantwert EANCV von einem zentralen Management-Netzwerkknoten den übrigen Netzwerkknoten des Netzwerks zur Verfügung gestellt, beispielsweise über eine Broadcast-Nachricht oder über Unicast-Nachrichten. Bei einer möglichen Ausführungsform sendet der Management-Netzwerkknoten den Konstantwert EANCV über eine Broadcast-Nachricht an alle übrigen Netzwerkknoten des Netzwerks. Bei einer alternativen Ausführungsform sendet der Management-Netzwerkknoten den Konstantwert EANCV jedem Netzwerkknoten über eine jeweilige Unicast-Nachricht. Bei einer weiteren Ausführungsform wird der NONCE-Wert N nicht nur in Abhängigkeit von einem Zählwert CTR und dem Konstantwert EANCV gebildet, sondern zusätzlich auch in Abhängigkeit von einer Sendeknotenadresse SA desjenigen Sendenetzwerkknotens, der die ausgesendete Nachricht F zu einem anderen Empfangsnetzwerkknotens des Netzwerks überträgt.

[0052] Nachdem ein NONCE-Wert N im Schritt S1 gebildet worden ist, erfolgt im Schritt S2 eine Ver- oder eine Entschlüsselung der in der Nachricht F übertragenen Daten jeweils mittels eines kryptographischen Schlüssels K, und mittels des gebildeten NONCE-Wertes N. Ein Sendenetzwerkknoten, der Daten geschützt zu einem Empfangsnetzwerkknoten übertragen möchte, verschlüsselt die Daten mittels eines kryptographischen Schlüssels K und des sendeseitig gebildeten NONCE-Wertes N.

[0053] Nach Empfang einer Nachricht F wird die Nachricht F durch den Empfangsknoten mittels eines entsprechenden kryptographischen Schlüssels K und des NONCE-Wertes wieder entschlüsselt.

[0054] Fig. 2 zeigt schematisch die Übertragung einer Nachricht bzw. eines Frames F innerhalb eines erfindungsgemäßen Netzwerks **1** von einem Sendeknoten **2-1** zu einem Empfangsknoten **2-2** des Netzwerks **1**. Das Netzwerk **1** kann aus einer Vielzahl von Netzwerkknoten **2** bestehen, die untereinander Frames F austauschen. Die Übertragung der Frames bzw. Nachrichten F erfolgt zwischen den Netzwerkknoten **2** des Netzwerks entweder direkt oder indirekt über andere Netzwerkknoten des Netzwerks. Bei den Netzwerkknoten **2** kann es sich beispielsweise um Netzwerkknoten handeln, die einen oder mehrere Sensoren enthalten. Diese Sensor-Netzwerkknoten übertragen die erfassten Messdaten der Sensoren in Nachrichten F bzw. Frames an anderen Netzwerkknoten zu deren Auswertung. Bei den Sensoren kann es sich um beliebige Sensoren, beispielsweise Temperaturmessfühler oder dergleichen handeln. Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens werden die Messdaten in Nachrichten bzw. Datenpaketen oder Frames F übertragen.

[0055] Fig. 3 zeigt ein mögliches Datenformat, wie es bei dem erfindungsgemäßen Verfahren eingesetzt werden kann. Der Frame F weist Header- bzw. Verwaltungsdaten HDR auf. Diese Header-Daten HDR enthalten Informationen über den Frame F, insbesondere über die Identität des Sendeknotens oder die Identität des Empfangsknotens. Wie in Fig. 3 dargestellt enthält der Header HDR unter Anderem eine Sendeknotenadresse SA, eine Empfangsknotenadresse EA sowie weitere Verwaltungsdaten. Bei der Sendeadresse SA und der Empfangsadresse EA kann es sich beispielsweise um eine MAC-Adresse handeln.

[0056] Bei dem erfindungsgemäßen Verfahren enthält der Header HDR zusätzlich einen Zählwert CTR, der beispielsweise durch einen in dem Sendeknoten **2-1** durch einen internen Zähler gebildet wird. Dieser

Zählwert CTR wird bei der Übertragung einer Nachricht F von dem Sendeknoten **2-1** zu den Empfangsknoten **2-2** aktualisiert, wobei die Aktualisierung in der Regel in einer Inkrementierung des Zählwertes CTR besteht. An die Header-Daten HDR schließen sich in dem Datenpaket bzw. dem Frame F Nutzdaten bzw. Payload-Daten an. Diese Nutzdaten sind beispielsweise verschlüsselte Daten von einem oder mehreren Sensoren des Sendeknotens **2-1**. Die Daten bzw. Messdaten des sendenden Knotens **2-1** geben beispielsweise den Ort bzw. die Koordinaten des Sendeknotens **2-1** sowie die dort herrschende Temperatur an. Die verschlüsselten Daten können aber auch Steuerdaten bzw. Steuerbefehlsdaten umfassen. Die Nutzdaten des in Fig. 3 dargestellten Frames F sind mit einem Schlüssel K und einem NONCE-Wert N verschlüsselt. Darüber hinaus kann die Nachricht bzw. der Frame F eine Prüfsumme CKS enthalten. Diese Prüfsumme kann eine digitale Signatur, eine Checksumme oder einen Authentisierungscode (Message Authentication Code) aufweisen.

[0057] Neben der Sendeadresse SA des Sendeknotens **2-1** bzw. der Sende-ID wird die Empfangsadresse EA des Empfangsknotens bzw. der Empfangs-ID mit dem aktualisierten Zählwert (TR) enthalten die Header-Daten HDR des in Fig. 3 dargestellten Frames F, gegebenenfalls zusätzliche Verwaltungsdaten, wie beispielsweise einen Typ des Frames (Type), eine Länge des Datenfeldes bzw. eine Menge der in dem Datenpaket enthaltenen Nutzdaten (length) und weitere Flags. Der Typ des Frames bzw. der Nachricht kann beispielsweise angegeben, ob es sich um einen Daten-Frame, ein Steuerkommando oder um einen Acknowledgement-Befehl handelt. Innerhalb des Headers HDR kann zum Beispiel angegeben werden, dass ein Sicherheitsmechanismus aktiviert ist (Security Enable) oder welche Protokollversion benutzt wird. Bei einer möglichen Ausführungsform des erfindungsgemäßen Verfahrens werden die in der Nachricht F übertragenen Daten durch einen CCM-Algorithmus kryptographisch verschlüsselt, wie beispielsweise in 802.15.4-2006 angegeben. Dieses Verschlüsselungsverfahren ermöglicht es, die Vertraulichkeit, die Integrität oder beides zu gewährleisten.

[0058] Der in Fig. 3 dargestellte Frame F bzw. die Nachricht N, die zwischen den Knoten **2** des Netzwerks **1** ausgetauscht werden, können drahtlos oder drahtgebunden übertragen werden. Eine drahtlose Kommunikation zwischen den Netzwerkknoten **2** bietet in vielen industriellen Anwendungen Vorteile. Die Vorteile umfassen beispielsweise geringe Installationskosten, eine flexible Installation der Netzwerkknoten **2** zur Vermeidung von mechanischem Verschleiß bei Kabeln oder Schleifkontakten und eine einfache Erweiterbarkeit des Netzwerks **1**. Das erfindungsgemäße Verfahren erlaubt eine kryptographisch geschützte Übertragung von Daten zwischen Netzwerkknoten **2** eines derartigen drahtlosen Netzwerks **1**, wobei ein Schutz insbesondere gegenüber wiedereingespielte Nachrichten bzw. Replay-Attacken gegeben ist.

[0059] Fig. 4 zeigt ein Blockschaltbild eines Netzwerkknotens **2** innerhalb des erfindungsgemäßen Netzwerks **1**. Das in Fig. 4 dargestellte Blockschaltbild stellt die Bildung eines NONCE-Wertes N in einem Sendeknotens **2-1** und die Verschlüsselung von Daten mit Hilfe eines kryptographischen Schlüssels K und des gebildeten NONCE-Wertes N dar. Der in Fig. 4 dargestellte Sendeknoten **2-1** enthält zwei Sensoren **3A**, **3B**, die Messdaten über eine Ein-/Ausgabeeinheit **4** an eine Verschlüsselungseinrichtung **5** liefern. Ein Sensorknoten **2** des erfindungsgemäßen Netzwerks **1** kann über einen oder auch eine beliebig hohe Anzahl von verschiedenen Sensoren **3** verfügen. Bei einer alternative Ausführungsform weist der Netzwerkknoten **2** keine Sensoren auf, sondern es werden andere Daten, die beispielsweise aus einem Speicher ausgelesen werden, verschlüsselt in einer Nachricht F zu einem anderen Netzwerkknoten **2** übertragen. Bei der in Fig. 4 dargestellten Verschlüsselungseinrichtung **5** kann es sich beispielsweise um einen Prozessor CPU handeln, der einen Verschlüsselungsalgorithmus ausführt. Der Verschlüsselungsalgorithmus ist beispielsweise ein CCM-Algorithmus. Als zugrundeliegende Blockchiffre kann dabei insbesondere der AES- oder DES-Algorithmus eingesetzt werden. Die Verschlüsselung der von der Ein-/Ausgabeeinheit **4** ausgegebenen Daten, die beispielsweise von den Sensoren **3** stammen, erfolgt mittels eines kryptographischen Schlüssels K, der aus einem Speicher **6** ausgelesen wird, und in Abhängigkeit von einem gebildeten NONCE-Wert N. Bei dem Speicher **6** kann es sich beispielsweise um einen nicht-flüchtigen Flash-Speicher handeln.

[0060] Der zur Verschlüsselung notwendige NONCE-Wert N wird durch eine Einheit **7** gebildet bzw. generiert. Diese Schaltung bzw. Einheit **7** bildet den NONCE-Wert N aus einem Zählwert CTR und aus einem Konstantwert EANCV. Bei einer möglichen Ausführungsform wird der NONCE-Wert N durch die Einheit **7** zusätzlich in Abhängigkeit von einer Senderadresse SA des Sendeknotens **2-1** gebildet. Wie man in Fig. 4 erkennen kann, enthält der Sendeknoten **2-1** einen internen Zähler **8**, der einen Zählwert CTR generiert, wobei der Zählwert bei der Übertragung bzw. beim Aussenden einer Nachricht F aktualisiert wird. Die Aktualisierung kann beispielsweise darin bestellen, dass der Zählwert CTR inkrementiert wird. Bei einer alternativen Ausführungsform kann die Aktualisierung des Zählwertes CTR auch durch Dekrementierung des Zählwertes erfolgen. In einer weiteren Ausführungsform kann die Aktualisierung des Zählwertes CTR auch durch Berechnen eine Zahlenfolge nach einer vorgegebenen Berechnungsvorschrift, z.

B. zur Berechnung einer Pseudozufallszahlenfolge, erfolgen. Die Sendeadresse SA des Sendeknotens **2-1** sowie der gemeinsame Konstantwert EANCV können, wie in Fig. 4 dargestellt, aus einem Speicher **9** ausgelesen werden. Bei dem Speicher **9** kann es sich beispielsweise um einen RAM-Speicher handeln. Die Einheit **7** bildet bei einer Ausführungsform einen NONCE-Wert N aus dem Zählwert CTR sowie aus dem Konstantwert EANCV. Bei einer alternativen Ausführungsform erfolgt die Bildung des NONCE-Wertes N zusätzlich in Abhängigkeit von der Sendeknotenadresse SA der Sendeknoten **2-1**, die aus dem Speicher **9** ausgelesen wird.

[0061] Bei einer möglichen Ausführungsform des erfindungsgemäßen Verfahrens wird der NONCE-Wert N durch die Einheit **7** durch Konkatenation bzw. Verletzung der Sendeknotenadresse SA des Sendenetzwerkknotens **2-1**, des gemeinsamen Konstantwertes EANCV und des Zählwertes CTR, der von dem internen Zähler **8** in dem der Sendenetzwerkknoten **2-1** erzeugt wird, gebildet.

[0062] Bei dieser Ausführungsform werden die jeweiligen Bitfolgen konkateniert bzw. aneinander gehängt.

N := SA|EANCV|CTR

[0063] Bei einer alternativen Ausführungsform wird der NONCE-Wert N durch die Einheit **7** mittels einer Hash-Funktion gebildet, beispielsweise MD5 oder SHA1, SHA-256. Die Hash-Funktion wird auf die Konkatenation der Sendeknotenadresse SA des Sendenetzwerkknotens **2-1**, des gemeinsamen Konstantwertes EANCV und des Zählwertes CTR angewendet.

N := HASH(SA|EANCV|CTR)

[0064] Bei alternativen Ausführungsformen können die Sendeknotenadresse SA, der Konstantwert EANCV und der Zählwert CTR in einer beliebigen anderen Reihenfolgen an konkateniert bzw. aneinandergehängt werden. Beispielsweise kann der NONCE-Wert auch wie folgt gebildet werden:

N := SA|CTR|EANCV oder

N := EANCV|SA|CTR usw.

[0065] Bei der Einheit **7** kann es sich um eine fest-verdrahtete Schaltung handeln, um den schaltungstechnischen Aufwand minimal zu halten. Bei einer alternativen Ausführungsform erfolgt die Bildung des NONCE-Wertes N durch die Einheit **7** durch Ausführen eines entsprechenden Programms zur Bildung eines NONCE-Wertes N, wobei dieses NONCE-Wert-Generierungsprogramm bei einer möglichen Ausführungsform konfigurierbar ist. Der gebildete NONCE-Wert N wird der Verschlüsselungseinheit **5** zur Verfügung gestellt. Die Verschlüsselungseinheit **5** kann ihrerseits eine fest-verdrahtete Schaltung sein oder aus einem Mikroprozessor bestehen. Bei einer möglichen Ausführungsform erfolgt die Bildung des NONCE-Wertes N und die Verschlüsselung durch den gleichen Mikroprozessor bei Ausführung entsprechender Prozeduren. Die Verschlüsselungseinheit **5** verschlüsselt die Daten, beispielsweise Sensor-Messdaten, mittels eines kryptographischen Schlüssels K und des von der Einheit **7** gebildeten NONCE-Wertes N. Die Verschlüsselung kann symmetrisch oder asymmetrisch erfolgen. Die verschlüsselten Daten werden anschließend als Nutzdaten in einen Frame F bzw. in ein Datenpaket eingepackt, wie es in Fig. 3 dargestellt ist. Dieser Frame F wird von einem Funk-Modul **10** des Knotens **2-1** über eine Sende-/Empfangsantenne **11** ausgestrahlt. Die Stromversorgung des Knotens **2-1** erfolgt, wie in Fig. 4 dargestellt, durch eine Stromversorgungseinheit **12**. Bei einer bevorzugten Ausführungsform weist der Knoten **2** des Netzwerkes **1** eine autonome Strom- bzw. Energieversorgung auf, beispielsweise eine Batterie, einen Akkumulator oder Solarzellen.

[0066] Der in dem Speicher **9** gespeicherte netzwerkweit eingesetzte Konstantwert EANCV ist bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens durch einen zentralen Managementknoten umkonfigurierbar. Erhält der in Fig. 4 dargestellte Knoten **2-1** über die Sende-Empfangsantenne **11** eine für ihn bestimmte Unicast-Nachricht oder eine Broadcast-Nachricht, wird der von einem Management-Netzwerkknoten erhaltene netzwerkweit einzusetzende Konstantwert EANCV von dem Funkmodul **10** in den Speicher **9** eingeschrieben. Anschließend kann der Sendeknoten **2-1** den aktuellen Konstantwert EANCV des Netzwerkes zur Verschlüsselung benutzen.

[0067] Der Konstantwert EANCV wird dabei auf allen Sensorknoten **2** des Netzwerkes **1** umkonfiguriert, d. h. es empfängt, speichert und verwendet jeder Sensorknoten **2** des Netzwerks **1** den neuen netzwerkweit eingesetzten Konstantwert EANCV.

[0068] Bei einer möglichen Ausführungsform erfolgt die Umkonfiguration des netzwerkweit eingesetzten Konstantwertes EANCV in festen, das heißt regelmäßigen Zeitabständen, beispielsweise täglich oder monatlich.

[0069] Bei einer alternativen Ausführungsform erfolgt die Umkonfiguration des gemeinsamen Konstantwertes EANCV, wenn die in dem Netzwerk **1** übertrage Datenmenge einen vorgegebenen einstellbaren Datenmengen-Schwellenwert überschreitet.

[0070] Bei einer alternativen Ausführungsform erfolgt die Umkonfiguration des gemeinsamen Kon-

stantwertes EANCV durch den Managementknoten bei Überschreitung einer vorgegebenen Anzahl von übertragenen Nachrichten F innerhalb des Netzwerkes **1**.

[0071] Bei einer weiteren möglichen Ausführungsform erfolgt die Umkonfiguration des netzwerkweit eingesetzten Konstantwertes EANCV beim Überschreiten einer vorgegebenen Anzahl von übertragenen Nachrichten F bei einem Knoten **2** innerhalb des Netzwerkes **1**.

[0072] Bei einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens erfolgt eine Umkonfiguration des gemeinsam eingesetzten Konstantwertes EANCV, wenn ein Zähler innerhalb des Netzwerkes **1** einen vorgegebenen Zählwert erreicht. Wird beispielsweise durch einen internen Zähler eines Sensorknotens **2** oder eines Gateways, das als Managementnetzwerkknoten dienen kann, ein vorgegebener Zählwert CTR erreicht, erfolgt die Umkonfiguration des Konstantwertes EANCV. Der Schwellenwert kann bei einer möglichen Ausführungsform je nach Anwendung eingestellt werden.

[0073] Bei einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens erfolgt eine Umkonfiguration des gemeinsamen Konstantwertes EANCV bei Eintritt eines vorgegebenen Ereignisses. Wird beispielsweise eine bestimmte Situation durch das Netzwerk **1** erkannt, etwa ein Sicherheitsalarm oder dergleichen, kann automatisch die Umkonfiguration des gemeinsamen Konstantwertes EANCV eingeleitet werden. Auf diese Weise ist es nicht möglich, ältere NONCE-Werte wieder einzuspiegeln oder fälschlicherweise einen fehlerfreien Zustand des Netzwerkes **1** bzw. fälschlicherweise einen Sonderzustand des Netzwerkes **1** vorzugegeben.

[0074] Bei einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens erfolgt die Umkonfiguration des Konstantwertes EANCV, wenn die verschlüsselt übertragenen Daten eine vorgegebene Bedingung erfüllen. Wenn beispielsweise in einem Sensornetzwerk **1** eine Temperaturänderung von mehr als 5 Kelvin erfasst wird, kann eine Umkonfiguration vorgenommen werden. Auf diese Weise können ältere Messwerte, zum Beispiel diejenigen, die mehr als 5 Kelvin Unterschied haben, von einem Angreifer nicht wiedereingespiegelt werden. Das bedeutet, dass ein maximaler Messfehler, den ein Angreifer durch wiedereingespiegelte Messnachrichten bewirken kann, begrenzt wird.

[0075] Der aktuelle bzw. umkonfigurierte EANCV-Wert wird bei einer möglichen Ausführungsform von einem zentralen Managementknoten des Netzwerkes **1** den Knoten **2** des Netzwerkes **1** zugewiesen. Dies kann beispielsweise durch eine Broadcast-Nachricht erfolgen. Alternativ werden die verschiedenen Netzwerkknoten **2** mit einer Unicast-Nachricht jeweils separat über den umkonfigurierten Konstantwert EANCV in Kenntnis gesetzt.

[0076] Bei einer alternativen Ausführungsform kann der gemeinsame Konstantwert EANCV den jeweiligen Netzwerkknoten in festen Zeitabständen automatisch inkrementiert bzw. um eins erhöht werden. Beispielsweise kann jeder Netzwerkknoten **2** täglich seinen EANCV um 1:00 Uhr nachts inkrementieren. Bei einer weitern Ausführungsform ist es anhand des EANCV-Wertes, welcher in von anderen Knoten **2** des Netzwerks **1** gesendeten Nachrichten F verwendet wird, ersichtlich, dass ein anderer Knoten **2** bereits auf einen aktualisierten EANCV-Wert gewechselt hat. In diesem Falle kann ein Empfangsknoten **2-2**, der erkennt, dass ein Sendeknoten **2-1** auf einen EANCV-Wert gewechselt hat, seinen EANCV ebenfalls auf den neuen Wert einstellen.

[0077] Bei einer weiteren Ausführungsvariante bilden die EANCV-Werte eine sogenannte Hash-Chain bzw. Hash-Kette. Dabei sind ein aktualisierter EANCV-Wert und ein bisheriger EANCV-Wert über eine Hash-Funktion, beispielsweise MD5, SHA-1, SHA-256 miteinander verbunden:

Hash(EANCV-neu) = EANCV-alt.

[0078] Da eine kryptographische Hash-Funktion nicht umkehrbar ist, kann dieser aus dem alten, bisherigen EANCV-Wert praktisch nicht bestimmt werden. Wenn der neue EANCV-Wert bekannt ist, kann durch Berechnen von dessen Hash-Wertes überprüft werden, ob der neue EANCV-Wert korrekt ist oder nicht. Die Übertragung des neuen Hash-Wertes an die Netzwerkknoten **2** ist daher gegen Manipulation geschützt.

[0079] Bei einer weiteren Ausführungsform des erfindungsgemäßen Verfahrens wird nach einem Einspielen des aktualisierten neuen EANCV-Wertes der bisherige EANCV-Wert für einen gewissen Zeitraum gespeichert und kann weiterhin verwendet werden. In einem Überlappungszeitraum kann auf diese Weise mit beiden EANCV-Werten kommuniziert werden. Auf diese Weise können auch Nachrichten mit Netzwerkknoten **2** ausgetauscht werden, die noch nicht über den aktualisierten EANCV-Wert verfügen. In diesem Überlappungszeitraum bzw. diese Übergangszeit kann ein Empfangsknoten **2-2** beide EANCV-Werte nutzen, um festzustellen, welcher EANCV-Wert zu einer erfolgreichen Entschlüsselung führt. Bei dieser Ausführungsvariante sind allerdings zwei Entschlüsselungsvorgänge notwendig, so dass der Rechenaufwand relativ hoch ist.

[0080] Bei einer alternativen Ausführungsform wird in einem Bit bzw. in einem Flag des Headers HDR der übertragenen Nachricht F angezeigt, ob der bisheri-

ge oder ein aktualisierter, EANCV-Wert zur Entschlüsselung zu benutzen ist. Auf diese Weise wird eindeutig angezeigt, welcher EANCV-Wert zur Entschlüsselung verwendet werden muss. Das Anzeige-Flag wechselt bei jedem Update bzw. bei jeder Umkonfiguration des netzwerkweit gemeinsam benutzten Konstantwertes EANCV.

[0081] Fig. 5 zeigt ein Blockschaltbild zur Darstellung eines Entschlüsselungsvorgangs innerhalb eines Empfangsknotens **2-2** des erfindungsgemäßen Netzwerkes **1**.

[0082] Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Netzwerkes **1** kann jeder Knoten **2** innerhalb des Netzwerkes **1** sowohl als Sendeknoten **2-1**, wie in Fig. 4 dargestellt, als auch als Empfangsknoten **2-2**, wie in Fig. 5 dargestellt, fungieren.

[0083] Bei der in Fig. 5 dargestellten Ausführungsform wird eine in dem Empfangsknoten **2-2** enthaltene Entschlüsselungseinheit (decrypt) durch die gleiche Einheit gebildet, wie die in Fig. 4 dargestellte Verschlüsselungseinheit, beispielsweise durch eine CPU bzw. einen Prozessor. Außerdem erfolgt die empfangsseitige Bildung des NONCE-Wertes N' durch die gleiche Einheit **7** wie die Bildung des NONCE-Wertes N auf Sendeseite. Bei dem in Fig. 5 dargestellten Ausführungsbeispiel empfängt der Empfangsknoten **2-2** über eine drahtlose Schnittstelle einen übertragenen Frame F bzw. eine Nachricht N, beispielsweise in dem in Fig. 3 dargestellten Datenformat. Aus den Header-Daten HDR des empfangenen Frames F werden durch eine Einheit **13** der übertragene Zählwert CTR sowie die Sendeadresse SA des Sendeknotens **2-1** extrahiert. Auf Grundlage der übertragenen Sendeknotenadresse SA-SK wird ein interner Zähler **14** innerhalb des Empfangsknotens **2-2** selektiert bzw. adressiert. Der interne Zähler **14** stellt einen Zähler CTR' bereit. Dieser selektierte Zählwert CTR' wird bei der in Fig. 5 dargestellten Ausführungsform durch eine Vergleichseinheit **15** mit dem in der Nachricht bzw. in dem Frame F übertragenen Zählwert CTR verglichen. Falls der übertragene Zählwert CTR aktueller ist als der selektierte Zählwert CTR' erzeugt der Komparator **15** ein Enable-Signal für die Einheit **7** zur Bildung eines empfangsseitigen NONCE-Wertes N'. Die Bildung des NONCE-Wertes N' im Empfangsknoten **2-2** erfolgt in gleicher Weise wie die Bildung des NONCE-Wertes N innerhalb des Sendeknotens **2-1** und ist in Zusammenhang mit Fig. 4 erklärt. Der empfangsseitig gebildete NONCE-Wert N' wird der Dekodiereinheit **5** bzw. der CPU zugeführt, welche die in der Nachricht F enthaltenen Daten mit Hilfe des Schlüssels K und dem empfangsseitig gebildeten NONCE-Wert N' entschlüsselt. Die entschlüsselten Daten können beispielsweise durch eine Datenverarbeitungseinheit **16** innerhalb des Empfangsknotens bearbeitet bzw. ausgewertet werden. Bei einer möglichen Ausführungsform bilden die Dekodiereinheit **5**, in der ein Dekodier- bzw. Entschlüsselungsalgorithmus ausgeführt wird, die Einheit **7** zur Bildung des NONCE-Wertes N' sowie die Datenverarbeitungseinheit **16** eine Einheit, beispielsweise in Form eines Mikroprozessors. Bei einer alternativen Ausführungsform ist die Entschlüsselungseinheit **5** eine speziell dafür vorgesehene fest-verdrahtete Schaltung.

[0084] Bei einer bevorzugten Ausführungsform des erfindungsgemäßen Verfahrens wird der sendeseitig oder empfangsseitig gebildete NONCE-Wert nur einmal mit demselben Schlüssel K verwendet. Dabei kann der Schlüssel K gewechselt werden, wenn ein möglicher Wertebereich des NONCE-Wertes ausgeschöpft ist. Der Sendeknoten **2-1** konstruiert bzw. bildet den NONCE-Wert N, um das zu übertragende Frame bzw. das übertragene Datenpaket kryptographisch zu schützen. Der Empfangsknoten **2-2** hat somit den selben NONCE-Wert aufgrund von Informationen, die in dem Datenpaket bzw. dem empfangenen Frame enthalten sind und gegebenenfalls auf Basis gespeicherter Zustandsinformationen, beispielsweise eines Zählwertes. Die Aktualität eines NONCE-Wertes N kann durch den Sendeknoten **2-1** auf unterschiedliche Weise gewährleistet werden und durch den Empfangsknoten **2-2** auf unterschiedliche Weise geprüft werden. Bei dem in Fig. 5 gezeigten Ausführungsbeispiel wird zur Gewährleistung der Aktualität des NONCE-Wertes N ein Zählwert CTR verwendet. Damit der Empfangsknoten die Aktualität eines NONCE-Wertes prüfen kann, speichert der Empfangsknoten **2-2** Informationen über den letzten empfangenen Zählwert ab und akzeptiert im Weiteren nur NONCE-Werte die aktueller sind als der gespeicherte Zählwert.

[0085] Bei der Konstruktion bzw. Bildung des NONCE-Wertes durch die Einheit **7** des Sendeknotens **2-1** oder des Empfangsknotens **2-2** können unterschiedliche Parameter eingehen. Diese Parameter können bei einer möglichen Ausführungsform neben einem Zählwert oder einer Knotenadresse auch ein Prioritätsfeld fassen. Als Zählwert eignet sich beispielsweise ein Frame-Counter der die Anzahl der übertragenen Frames F mitzählt.

[0086] Das erfindungsgemäße Verfahren zur kryptographisch geschützten Übertragung von Daten zwischen Netzwerkknoten **2** eines Netzwerks **1** eignet sich insbesondere auch für Netzwerke **1**, die über keine synchronisierte Uhrzeit verfügen. Beispielsweise eignet sich das erfindungsgemäße Verfahren insbesondere für ein Wireless-Sensor-Network WSN, das heißt für ein Netzwerk, das aus Sensorknoten besteht in denen einen synchronisierte Uhrzeitinformation nicht vorliegt.

[0087] Die Bitbreite des Zählwertes CTR, der zur

Prüfung der Aktualität eines NONCE-Wertes N herangezogen wird, wird vorzugsweise relativ breit gewählt, beispielsweise 32, 48 oder 64 Bit. Der Grund hierfür besteht darin, dass je breiter der Zähler bzw. je größer der Zählerwertebereich desto seltener muss der Schlüssel K ermittelt werden und desto seltener ist eine Neukonfiguration des Schlüssels K notwendig. Die Bitbreite des Zählerwertes CTR kann jedoch auch relativ klein gewählt werden, beispielsweise 4, 8 oder 16 Bit. Dies hat den Vorteil, dass nur wenige Bits für den verwendeten Zählerwertes CTR gespeichert und insbesondere übertragen werden müssen.

[0088] Die Verschlüsselung von Daten kann mit Hilfe des Schlüssels K und des gebildeten NONCE-Wertes N mit unterschiedlichen Verschlüsselungsalgorithmen erfolgen. Beispielsweise können die Daten kryptographisch mittels eines AES- oder DES-Algorithmus verschlüsselt werden, um den Frame F vor Manipulationen zu schützten. Vorzugsweise werden diese in einem CCM-Modus verwendet.

[0089] Der zur Bildung des NONCE-Wertes N herangezogene Konstantwert EANCV ist vorzugsweise netzwerkweit gültig. Das bedeutet, dass alle Netzwerkknoten des Netzwerkes **1** den gleichen EANCV-Wert zur Ver- und Entschlüsselung verwenden. Bei einer Variante wird der Konstantwert EANCV einer Teilgruppe der Knoten bzw. einer Teilmenge der Netzwerkknoten **2** zur Kommunikation untereinander zugewiesen.

[0090] Bei dem in einer Verschlüsselung eingesetzten kryptographischen Schlüssel K kann es sich um einen beliebigen Schlüssel handeln. Bei dem Schlüssel kann es sich beispielsweise um einen Netzwerkschlüssel (network key) handeln, der allen Netzwerkknoten **2** des Netzwerks **1** bekannt ist. Bei einer alternativen Ausführungsform ist der verwendete Schlüssel ein Verbindungsschlüssel (link key), der zwei direkt benachbarten Netzwerkknoten des Netzwerkes **1** bekannt ist. Bei einer weiteren Ausführungsform kann es sich bei dem Schlüssel K um einen Ende-zu-Ende-Schlüssel (end-to-end-key) handeln, der an den Endpunkten bzw. Endknoten der Kommunikation beispielsweise zwei Sensorknoten oder einem Sensorknoten und einem Gateway-Knoten bekannt ist. Bei weiteren Ausführungsvarianten ist der Schlüssel K ein Broadcast-Schlüssel oder ein Multicast-Schlüssel. Der bei der Verschlüsselung eingesetzte NONCE-Wert N kann durch Konkatenation von Bitfolgen verschiedener Parameter mit dem Konstantwert EANCV gebildet werden, beispielsweise durch Konkatenation des Konstantwertes EANCV mit einem Zählwert CTR und einer Senderknotenadresse SA. Bei einer möglichen Ausführungsform ist die Bitbreite des gebildeten NONCE-Wertes N variabel. Falls die Länge bzw. Bitbreite des EANCV-Wertes zu groß ist, beispielsweise falls textuelle Zeichenketten beliebiger Länge verwendet werden, kann mit Hilfe einer Hash-Funktion ein NONCE-Wert N mit einer fest vorgegebenen Länge berechnet werden.

[0091] Der jeweils in dem Netzwerk bzw. in einem Teilnetzwerk aktuell gültige Konstantwert EANCV wird bei einer bevorzugten Ausführungsform durch einen zentralen Managementknoten den Netzwerkknoten **2** des Netzwerkes **1** zugewiesen, wobei es sich bei dem Managementknoten beispielsweise um ein Gateway, einen Netzwerkmanagementserver (network manager) oder um einen Sicherheitsserver (security server, security manager) handelt. Die Zuweisung dieses EANCV-Wertes an die verschiedenen Knoten **2** des Netzwerkes **1** durch den Managementknoten erfolgt ebenfalls kryptographisch-geschützt.

[0092] Das erfindungsgemäße Verfahren bietet einen Schutz gegen sogenannte Replay-Attacken. Ein in der Vergangenheit übertragener Frame F, der durch einen Dritten abgehört und von diesem Dritten eingespielt wird, kann bei dem erfindungsgemäßen Übertragungsverfahren erkannt werden. Der eingespielte Frame F, der unter Verwendung eines nicht-aktuellen EANCV-Wertes generiert wurde, wird durch den Empfangsknoten **2-2** nicht akzeptiert. Ein zusätzlicher Schutz gegen Replay-Attacken wird mit Hilfe des mitübertragenen Zählwertes CTR erreicht. Dabei speichert der Empfangsknoten Informationsdaten über den zuletzt von einem Sendeknoten **2-1** empfangenen Zählwert CTR. In dem erfindungsgemäßen Verfahren wird der Zählwert CTR vorteilhafterweise aus einem relativ kleinen Wertebereich entnommen, beispielsweise 4, 8 oder 16 Bit, da der Zählwert CTR nur bezüglich jedes Konstantwertes EANCV eindeutig sein muss.

[0093] Bei dem in Fig. 6 dargestellten Beispielnetzwerk können 6 Sensorknoten **2** mit ein Gatewayknoten **2-0** über eine Funkschnittstelle kommunizieren. In dem in Fig. 6 dargestellten Ausführungsbeispiel stellt der Gatewayknoten **2-0** einen netzwerkweit eingesetzten Konstantwert EANCV den übrigen Netzwerkknoten **2-1** bis **2-6** zur Verfügung. Die Sensorknoten **2-1**, **2-3**, **2-4**, **2-5**, **2-6** weisen jeweils mindestens einen Sensor zur Erfassung von Messdaten, beispielsweise einer Umgebungstemperatur auf. Diese Messdaten werden verschlüsselt und als Frames F zur Auswertung der Messdaten übertragen. Der EANCV-Wert wird vorzugsweise von dem zentralen Managementknoten, das heißt durch den Gatewayknoten **2-0** des drahtlosen Sensornetzwerkes **1** an die übrigen Knoten **2-1** bis **2-6** übermittelt, die den EANCV-Wert zur weiteren Verwendung speichern. Die Übermittlung des EANCV-Wertes erfolgt manipulationssicher. Dies kann beispielsweise durch eine geschützte Übertragung zwischen dem zentralen Gateway **2-0** und den Sensorknoten **2-1** bis **2-6** geschehen. Alternativ stellt die Verbindung einen

Hash-Chain dar, bei der ein Hash-Wert des aktualisierten EANCV-Wertes von dem bisherigen EANCV-Wert abgeleitet wird.

[0094] Die Fig. 7A, Fig. 7B zeigen verschiedene Alternativen zur Übermittlung eines EANCV-Wertes von einem Managementknoten **2-0** zu übrigen Netzwerkknoten. Bei der in Fig. 7A dargestellten Alternative wird der EANCV-Wert von dem Gatewayknoten **2-0** jeweils mit einer Unicast-Nachricht (assign) separat an die verschiedenen Sensorknoten **2-1** bis **2-6** des Netzwerkes **1** übertragen. Dies bedeutet, dass jeder Sensorknoten **2-1** bis **2-6** separat den aktuellen EANCV-Wert erhält.

[0095] In der in Fig. 7B dargestellten Alternative erfolgt die Übermittlung des EANCV-Wertes mittels einer Broadcast- bzw. einer Multicast-Nachricht. Bei dieser Übermittlungsart wird der aktuelle EANCV-Wert von dem Gatewayknoten **2-7** über Zwischenknoten weitergeleitet. Dabei kann das Netzwerk **1** geflutet werden, so dass alle Sensorknoten die Zuweisungsnachricht mit dem aktuellen EANCV-Wert erhalten.

[0096] Fig. 8 zeigt ein weiteres Ausführungsbeispiel des erfindungsgemäßen Netzwerkes **1**. Bei diesem Ausführungsbeispiel handelt es sich um einen Sensornetzwerk mit Multi-Hop-Mesh-Topologie.

[0097] Fig. 9 zeigt ein weiteres Ausführungsbeispiel des erfindungsgemäßen Netzwerkes **1** mit einer Multi-Hop-Netzwerk-Topologie, die eine Baumstruktur aufweist.

[0098] Fig. 10 zeigt ein weiteres Ausführungsbeispiel des erfindungsgemäßen Netzwerkes **1** mit einer Single-Hop-Netzwerk-Topologie bzw. einer Sternstruktur.

[0099] Bei den in Fig. 8–Fig. 10 dargestellten Ausführungsbeispielen werden die Netzwerkknoten **1** durch Sensorknoten gebildet, die jeweils über mindestens einen Sensor verfügen. Das erfindungsgemäße Verfahren ist jedoch nicht auf die Übertragung von Nachrichten zwischen Sensorknoten **2** beschränkt, vielmehr können die Netzwerkknoten auch Aktoren bzw. eine Kombination aus Sensoren und Aktoren aufweisen. Bei einer möglichen Ausführungsform ist das Gateway **2-0**, wie es in den Fig. 6–Fig. 10 dargestellt ist, mit einem Computernetzwerk verbunden, beispielsweise einem Intranet oder einem Fertigungsnetzwerk. Bei einer möglichen Ausführungsform können auch mehrere Gateways vorhanden sein.

[0100] Das erfindungsgemäße Netzwerk **1** ist zudem nicht auf drahtlose Netzwerke beschränkt. Die Nachrichten F zwischen verschiedenen Netzwerkknoten **2** des Netzwerks **1** können auch drahtgebunden über eine Leitung übertragen werden.

[0101] In dem erfindungsgemäßen Netzwerk **1** wird derselbe EANCV-Wert zur Kommunikation zwischen den Knoten **2** verwendet. Dabei wird in den verschiedenen Knoten **2** jeweils nur wenig Speicherplatz benötigt, weil nur ein gemeinsamer EANCV-Wert gespeichert werden muss, unabhängig von der Anzahl von Kommunikationspartnern und von verwendeten Schlüsseln. So muss beispielsweise bei dem erfindungsgemäßen Verfahren nicht je ein Wert je Kommunikationspartner oder je Schlüssel oder je Kombination aus Kommunikationspartner und Schlüssel gespeichert werden. Somit ist es möglich, eine große effektive NONCE-Länge bei gleichzeitig geringen zu speichernden Datenumfang zu erreichen. Dadurch wird die Anforderung nach einem Re-Keying vermieden bzw. ein Re-Keying muss nur noch selten durchgeführt werden. Dies ermöglicht auch, die Zähler-Werte-Bereich relativ klein zu halten.

Patentansprüche

1. Verfahren zum kryptographisch geschützten Übertragung von Daten zwischen Netzwerkknoten (**2**) eines Netzwerkes (**1**), wobei zur Übertragung der Daten in einer Nachricht (F) die folgenden Schritte ausgeführt werden:
a) Bilden eines NONCE-Wertes (N), aus einem Zählwert (CTR), welcher bei der Übertragung der Nachricht (F) aktualisiert wird, und aus einem Konstantwert (EANCV), welcher den Netzwerkknoten (**2**) des Netzwerkes (**1**) gemeinsam zur Verfügung gestellt wird; und
b) Ver- und Entschlüsseln der in der Nachricht (F) übertragenen Daten mittels eines kryptographischen Schlüssels (K) und des gebildeten NONCE-Wertes (N).

2. Verfahren nach Anspruch 1, wobei der gemeinsame, netzwerkweit eingesetzte Konstantwert (EANCV) von einem zentralen Management-Netzwerkknoten (**2-0**) den übrigen Netzwerkknoten (**2-i**) des Netzwerks (**1**) bereitgestellt wird.

3. Verfahren nach Anspruch 1 oder 2, wobei der NONCE-Wert (N) zusätzlich in Abhängigkeit von einer Sendeknotenadresse (SA) desjenigen Sendenetzwerkknotens (**2-1**) gebildet wird, der die Nachricht (F) zu einem anderen Empfangsnetzwerkknoten (**2-2**) des Netzwerks (**1**) überträgt.

4. Verfahren nach Anspruch 2, wobei der gemeinsame Konstantwert (EANCV) von dem zentralen Management-Netzwerkknoten (**2-0**) durch Aussenden einer Broadcast-Nachricht oder durch Aussenden von Unicast-Nachrichten an die Netzwerkknoten (**2-i**) des Netzwerks (**1**) übertragen wird.

5. Verfahren nach Anspruch 2 oder 4, wobei der

gemeinsame Konstantwert (EANCV) von dem zentralen Management-Knoten (**2-0**) umkonfigurierbar ist.

6. Verfahren nach Anspruch 5, wobei eine Umkonfiguration des gemeinsamen Konstantwertes (EANCV) in festen Zeitabständen, nach Überschreiten einer vorgegebenen übertragenen Datenmenge, nach Überschreiten einer vorgegebenen Anzahl von übertragenen Nachrichten (F), nach Erreichen eines vorgegebenen Zählwertes bei einem der Netzwerkknoten (**2-i**) des Netzwerks (**1**), beim Eintritt eines vorgegebenen Ereignisses, oder bei einer Übertragung von Daten, die eine vorgegebene Bedingung erfüllen, erfolgt.

7. Verfahren nach Anspruch 3, wobei der NONCE-Wert (N) durch Konkatenation der Sendeknotenadresse (SA) des sendenden Netzwerkknotens (**2-1**), des gemeinsamen Konstantwertes (EANCV) und des Zählwertes (CTR), der von einem internen Zähler (**8**) des Sendenetzwerkknotens (**2-1**) erzeugt wird, gebildet wird.

8. Verfahren nach Anspruch 3, wobei der NONCE-Wert (N) durch eine Hash-Funktion der Konkatenation der Sendeknotenadresse (SA) des Sendenetzwerkknotens (**2-1**), des gemeinsamen Konstantwertes (EANCV) und des Zählwertes (CTR), der von einem internen Zähler (**8**) des Sendenetzwerkknotens (**1-2**) erzeugt wird, gebildet wird.

9. Verfahren nach einem der vorangehenden Ansprüche 1–8, wobei das Verschlüsseln und Entschlüsseln der in der Nachricht übertragenen Daten durch einen CCM-Algorithmus erfolgt.

10. Verfahren nach einem der Ansprüche 3–9, wobei die übertragene Nachricht (F) Header-Daten (HDR), welche eine Sendeknotenadresse (SA), eine Empfangsknotenadresse (EA) und den aktuellen Zählwert (CTR) des Sendenetzwerkknotens (**2-1**) aufweisen, und Nutzdaten (PL), welche die verschlüsselten Daten aufweisen, umfasst.

11. Verfahren nach Anspruch 10,
wobei der Empfangsnetzwerkknoten (**2-2**) den in der Nachricht (F) übertragenen Zählwert (CTR) des Sendenetzwerkknotens (**2-1**) mit einem anhand der in der Nachricht (F) übertragenen Sendeknotenadresse (SA) selektierten Zählwert (CTR') eines internen Zählers (**14**) des Empfangsnetzwerkknotens (**2-2**) vergleicht, und aus dem übertragenen Zählwert (CTR), aus dem gemeinsamen Konstantwert (EANCV) und aus der übertragenen Sendeknotenadresse (SA) einen empfangsseitigen NONCE-Wert (N') bildet, falls der übertragene Zählwert (CTR) aktueller ist als der selektierte Zählwert (CTR'),
wobei der empfangsseitig gebildete NONCE-Wert (N') und ein in dem Empfangsnetzwerkknoten (**2-2**) gespeicherter Schlüssel (K) zur Entschlüsselung der in der Nachricht (F) verschlüsselt übertragenen Daten benutzt werden.

12. Verfahren nach einem der vorangehenden Ansprüche 3–9, wobei die Nachricht (F) über eine Funkschnittstelle von dem Sendenetzwerkknoten (**2-1**) zu dem Empfangsnetzwerkknoten (**2-2**) übertragen wird.

13. Netzwerk (**1**) bestehend aus mehreren Netzwerkknoten (**2**), die untereinander Daten in Nachrichten (F) übertragen, wobei jeder Netzwerkknoten (**2**) aufweist:
a) eine Einheit (**7**) zum Bilden eines NONCE-Wertes (N), aus einem Zählwert (CTR), welcher bei der Übertragung einer Nachricht (F) aktualisiert wird, und aus einem Konstantwert (EANCV), welcher den Netzwerkknoten (**2**) des Netzwerkes (**1**) gemeinsam zur Verfügung gestellt wird; und
b) eine Einheit (**5**) zur Ver- und Entschlüsselung der in der Nachricht (F) übertragenen Daten mittels eines kryptographischen Schlüssels (K) und des gebildeten NONCE-Wertes (N).

14. Netzwerk nach Anspruch 13, wobei das Netzwerk (**1**) einen zentralen Management-Netzwerkknoten (**2-0**) aufweist, der den gemeinsamen Konstantwert (EANCV) den übrigen Netzwerkknoten (**2-i**) des Netzwerkes (**1**) zur Verfügung stellt.

15. Netzwerk nach Anspruch 13 oder 14, wobei die Netzwerkknoten (**2**) jeweils mindestens einen Sensor (**3**) aufweisen.

16. Computerprogramm mit Programmbefehlen zur Durchführung des Verfahrens nach Ansprüchen 1–12.

17. Datenträger, der das Computerprogramm nach Anspruch 16 speichert.

Es folgen 6 Blatt Zeichnungen

Anhängende Zeichnungen

FIG 1

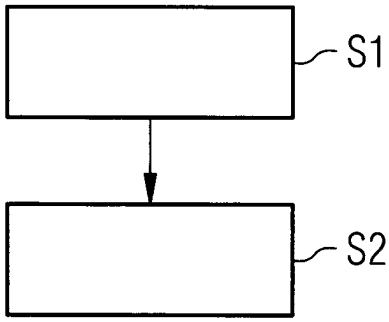


FIG 2

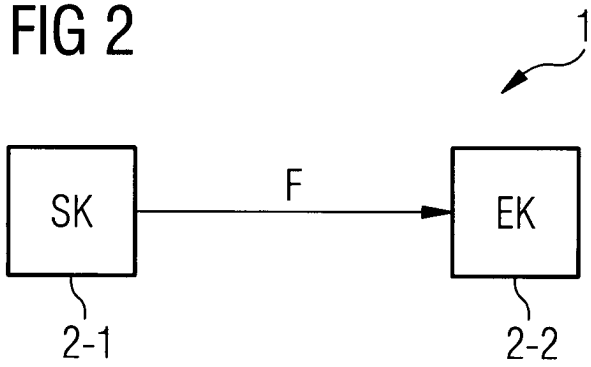


FIG 3

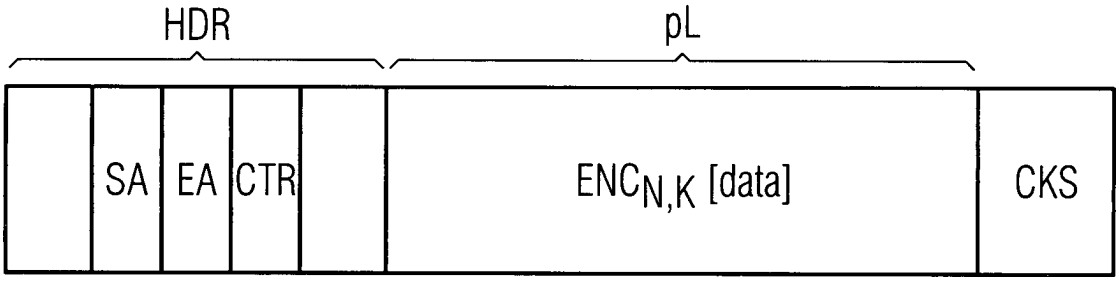


FIG 4

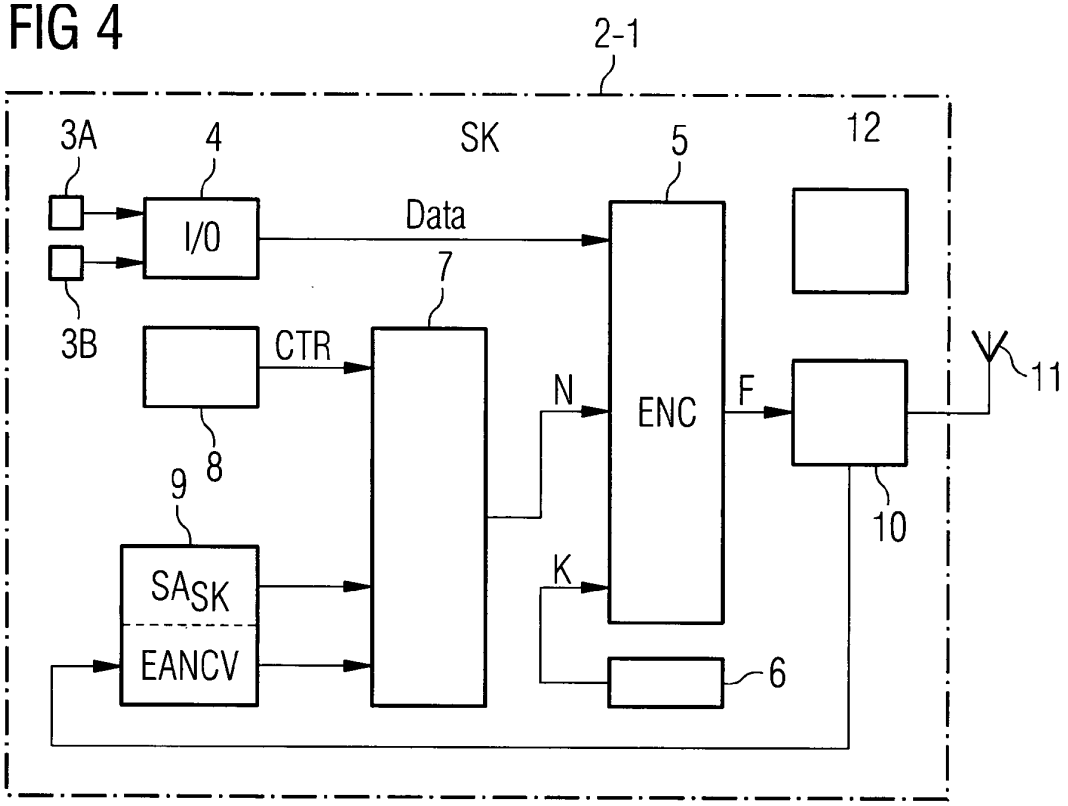

2-1
3A
4
SK
5
12
I/O
Data
3B
7
CTR
N
ENC
F
11
8
9
10
SASK
K
EANCV
6

FIG 5

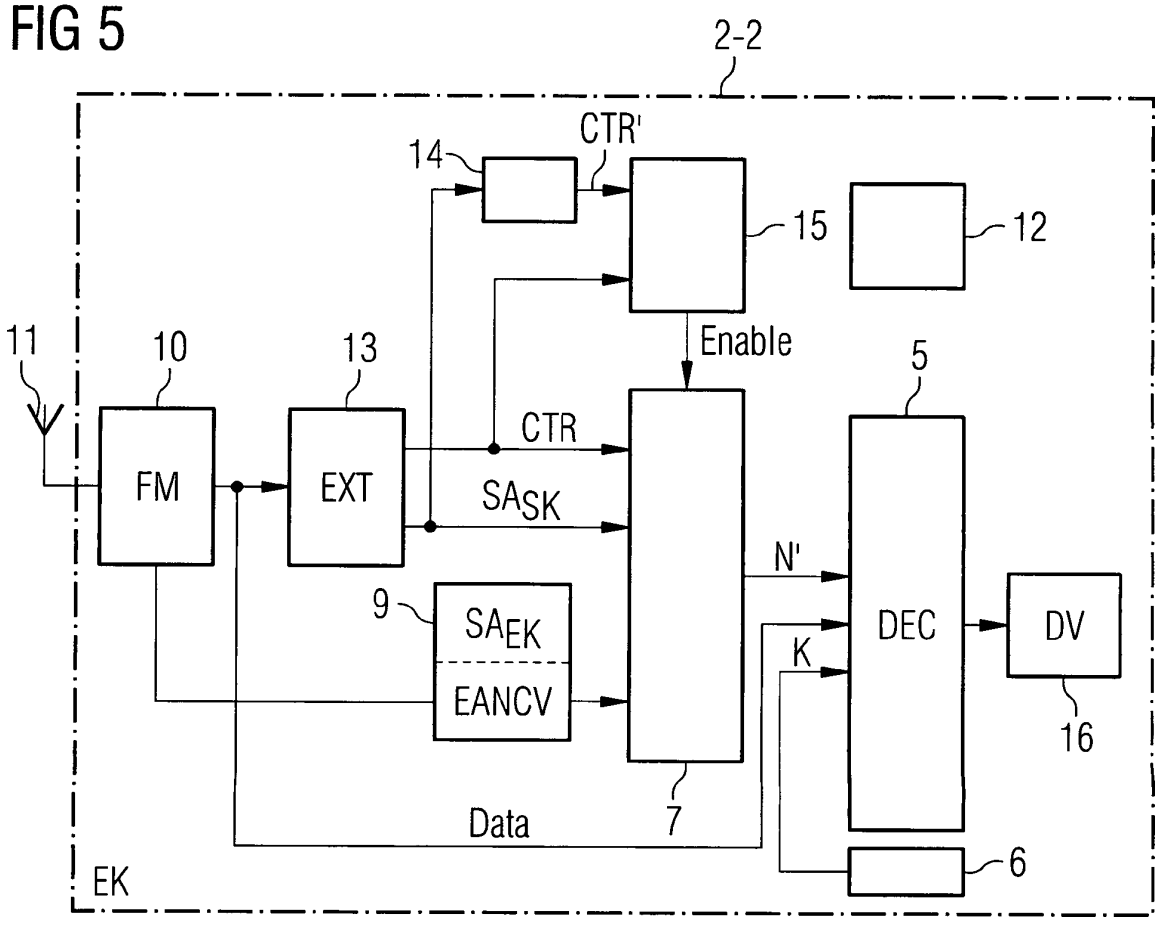

2-2
CTR'
14
15
12
Enable
11
10
13
5
CTR
FM
EXT
SASK
N'
9
SAEK
DEC
DV
K
EANCV
16
Data
7
6
EK

FIG 6

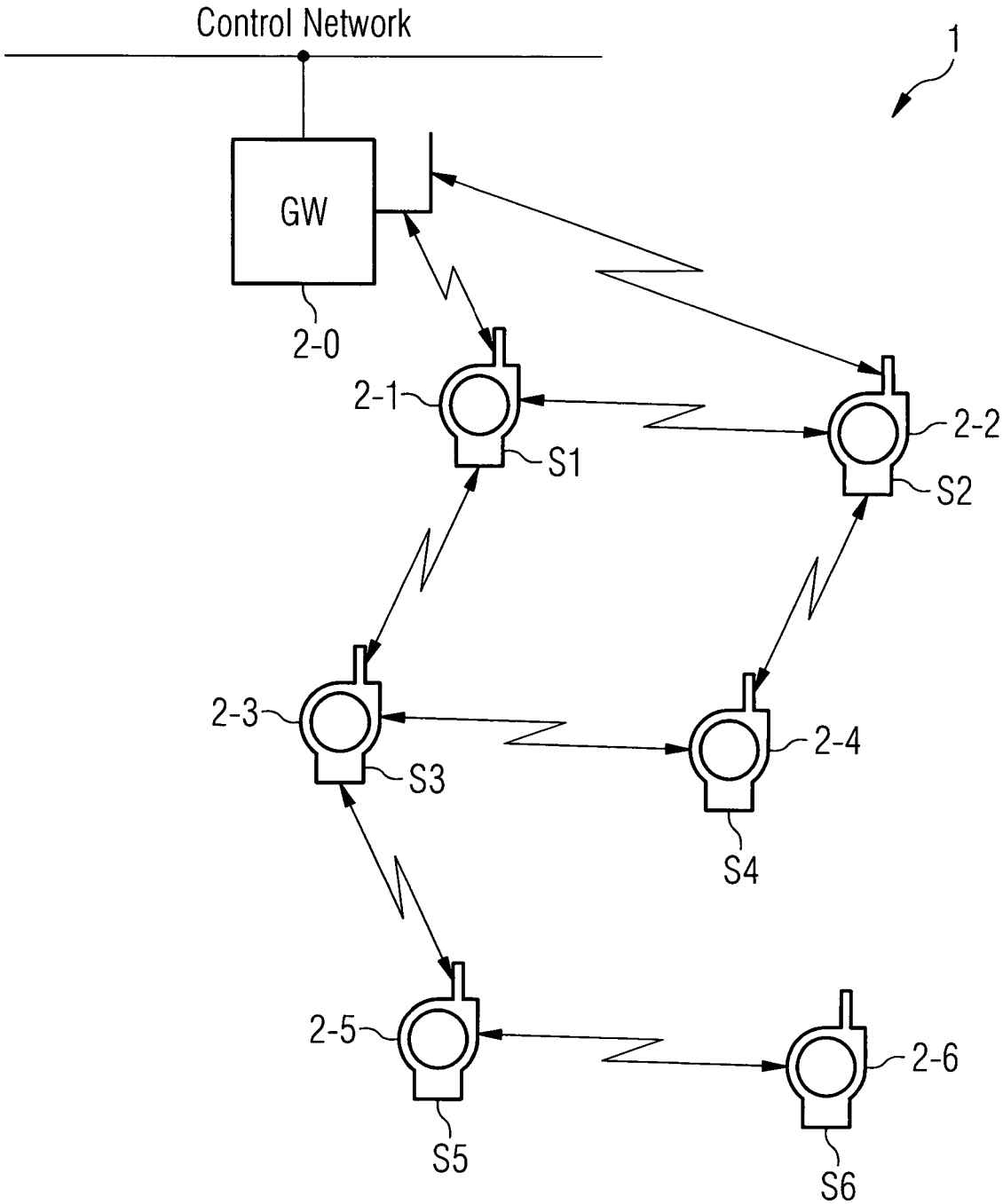


FIG 7A

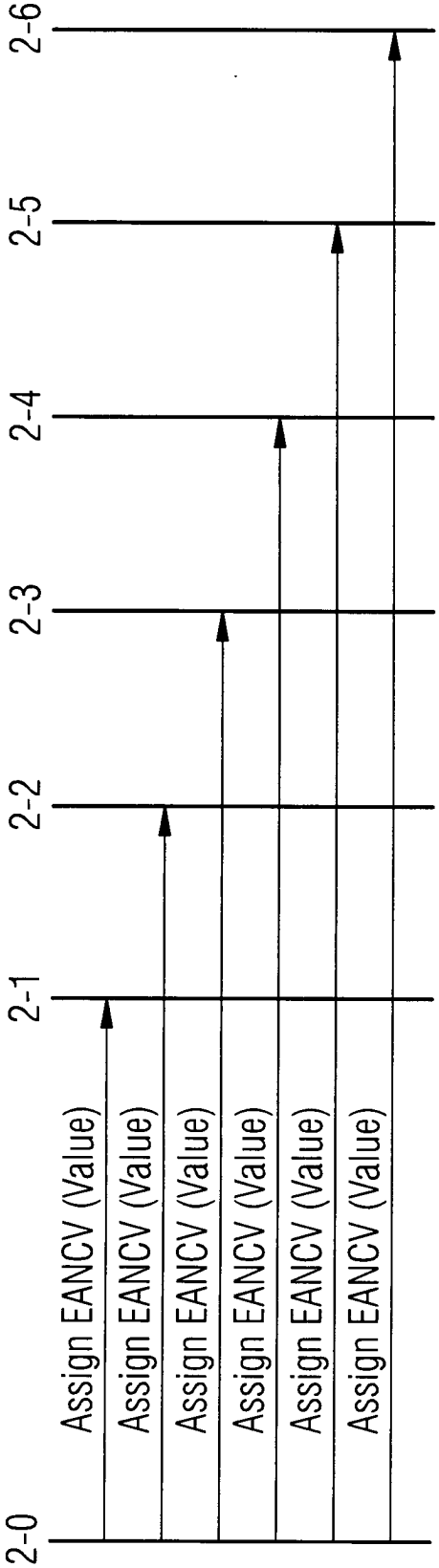

2-0
2-1
2-2
2-3
2-4
2-5
2-6
Assign EANCV (Value)
Assign EANCV (Value)
Assign EANCV (Value)
Assign EANCV (Value)
Assign EANCV (Value)
Assign EANCV (Value)

FIG 7B

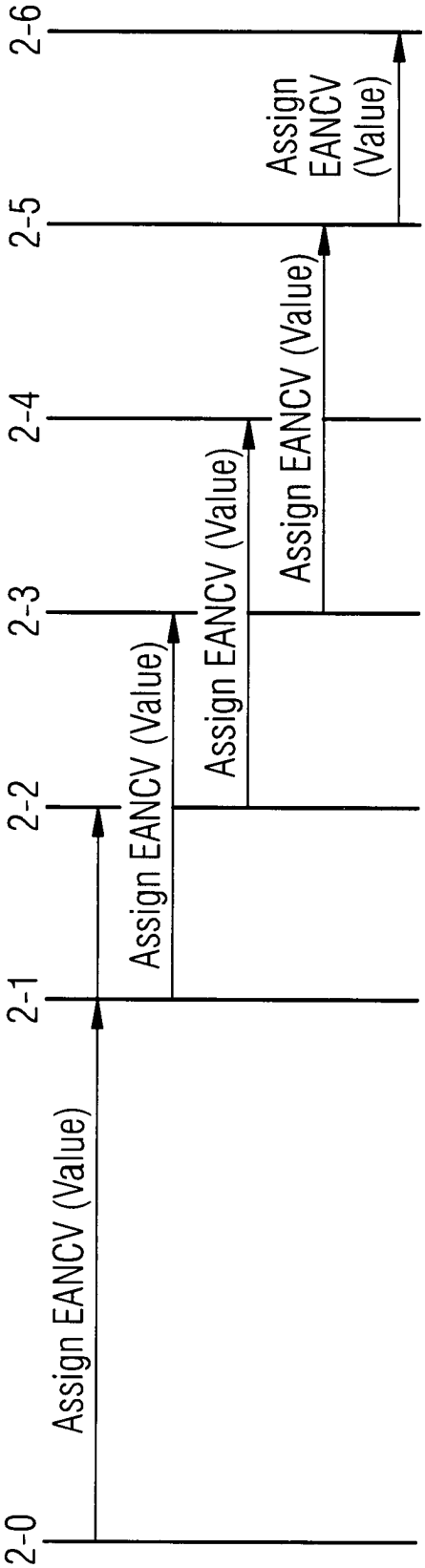

2-0
2-1
2-2
2-3
2-4
2-5
2-6
Assign EANCV (Value)
Assign EANCV (Value)
Assign EANCV (Value)
Assign EANCV (Value)

FIG 8

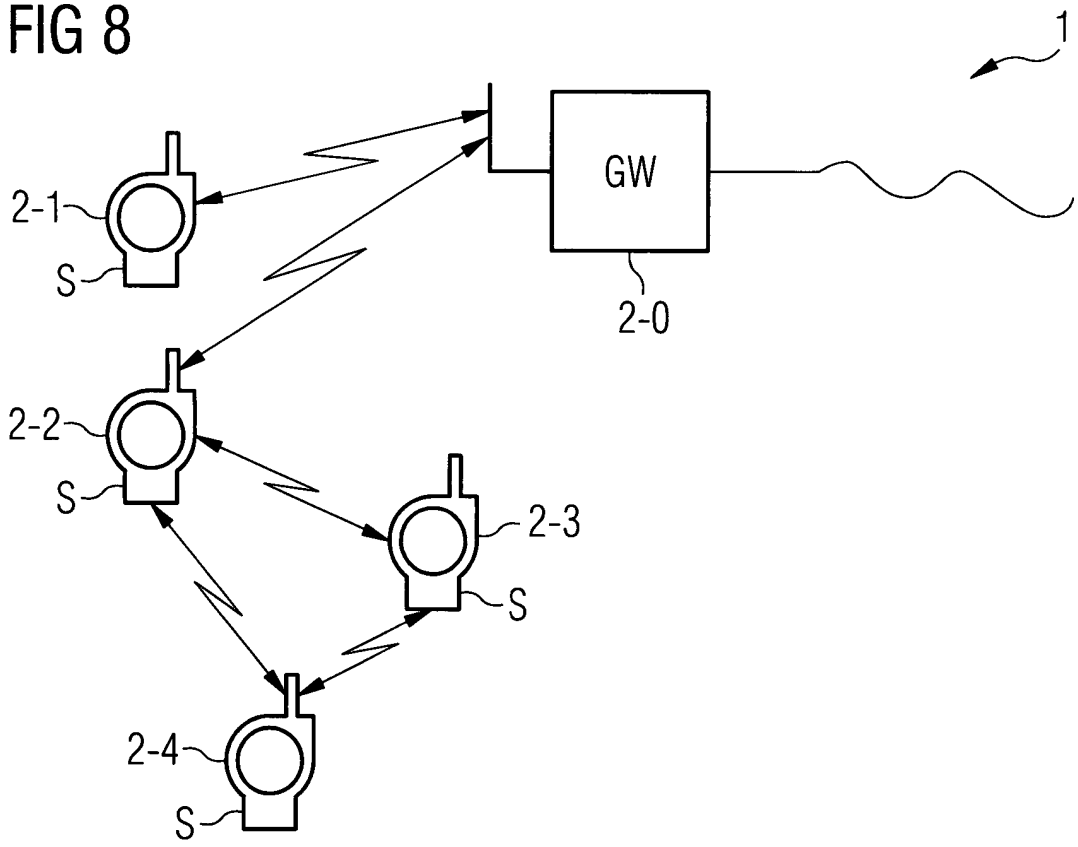


FIG 9

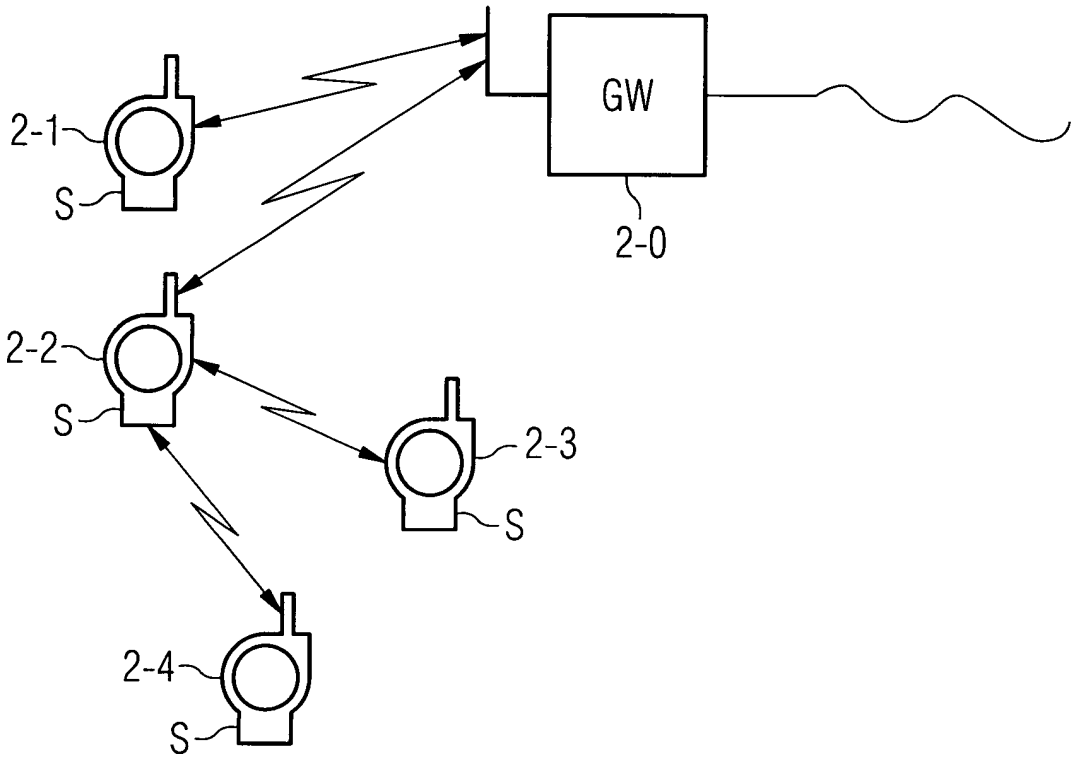


FIG 10