(19) Deutsches Patent- und Markenamt

(10) **DE 10 2020 216 122 A1** 2021.06.17

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2020 216 122.4**
(22) Anmeldetag: **17.12.2020**
(43) Offenlegungstag: **17.06.2021**

(51) Int Cl.: ***H03M 13/31*** (2006.01)

(30) Unionspriorität:
101567 **17.12.2019** **LU**

(71) Anmelder:
Universität Bremen, Körperschaft des öffentlichen Rechts, 28359 Bremen, DE

(74) Vertreter:
RCD-Patent Giesen, Schmelcher & Griebel Patentanwälte Partnerschaftsgesellschaft mbB, 52134 Herzogenrath, DE

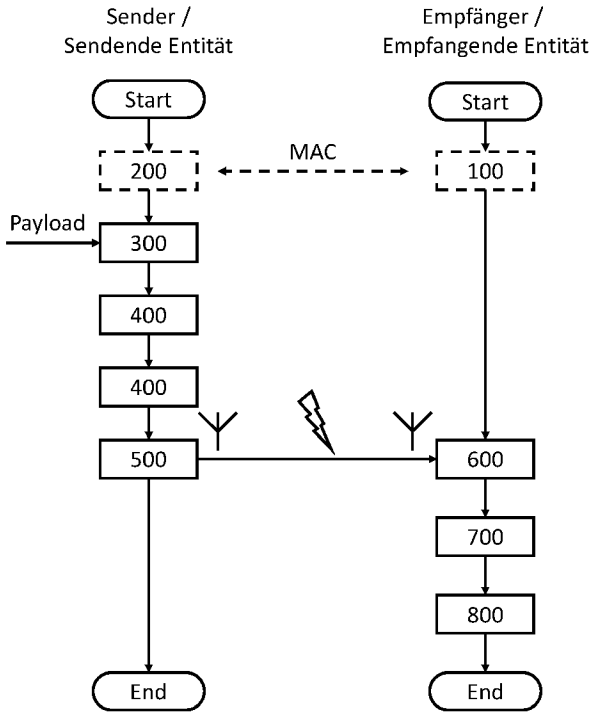
(72) Erfinder:
Demel, Johannes, 28211 Bremen, DE;
Bockelmann, Carsten, Dr. Ing., 28832 Achim, DE;
Dekorsy, Armin, Prof. Dr. Ing., 28357 Bremen, DE

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **VERFAHREN FÜR EINE SENDENDE ENTITÄT UND VERFAHREN FÜR EINE EMPFANGENDE ENTITÄT IN EINER NETZWERKUMGEBUNG**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren für ein System aufweisend eine sendende nd eine empfangende Entität in einer Netzwerkumgebung, wobei das Verfahren für eine sendende Entität zu empfangenen Nutzlastinformationen für einen spezifischen Empfänger einen Nachrichtauthentifizierungscodes hinzufügt. Die empfangende Entität empfängt die kodierte Information und dekodiert diese. Die empfangende Entität bestimmt, ob die dekodierte Information basierend auf dem Schlüssel des Empfängers authentifiziert werden kann, und falls die Authentifizierung gegeben ist, weiterleiten der dekodierten Information oder von Teilen davon zur weiteren Verarbeitung, wobei das Dekodieren derart auf einer Kandidatenliste basiert, dass Kandidaten der Dekodierung der Bestimmung unterliegen bis ein erster Kandidat authentifiziert wird oder das Ende der Liste von Kandidaten erschöpft ist, wobei das Kodieren ein polares Kodieren oder ein Turbokodieren ist, wobei Kodieren FEC-Eigenschaften bereitstellt, und wobei Dekodieren auf einem Arikan Successive Cancellation Decoder basiert.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren für eine sendende Entität und ein Verfahren für eine empfangende Entität in einer Netzwerkumgebung.

Hintergrund

[0002] Es ist bekannt, dass mit dem laufenden Trend, Vorrichtungen mit Kommunikationsfähigkeiten bereitzustellen, Daten, die von diesen Vorrichtungen ausgehen, in Richtung eines oder mehrerer Empfänger gesendet werden.

[0003] In der Kundeneinrichtung ist dies als Smart-Vorrichtungen bekannt und wird häufig im Kontext von Smart-Heimen angeführt. Dort stellen unterschiedliche Vorrichtungen, wie etwa Energiequellen oder Energieverbraucher, Daten zu ihrem aktuellen Status bereit. Eine Photovoltaikanordnung kann beispielsweise Daten in Bezug auf tatsächliche Stromerzeugung bereitstellen, ob eine Platte weniger Energie als andere liefert oder nicht, während eine Heizung Daten in Bezug auf eine aktuelle Temperatur für Heiz- oder Warmwasserzwecke, tatsächlichen Energieverbrauch und dergleichen bereitstellen kann, Temperatursensoren und Windsensoren können tatsächliche Messdaten bereitstellen. Sensoren und Akteure, die an unterschiedlichen Standorten angeordnet sind, stellen Statusdaten bereit und/oder empfangen Daten in Bezug auf bestimmte Operationen. Schirme können beispielsweise auf ein bestimmtes Niveau gesteuert werden.

[0004] In der Industrie ist ein ähnliches Szenario als Industry 4.0 bekannt. Darin ist die Kommunikation von Maschinen miteinander auch als Machine-to-Machine-Kommunikation, auch M2M genannt, bekannt.

[0005] Im Transportwesen gewinnt autonomes Fahren Interesse. Man geht davon aus, dass in solch einem Bereich Fahrzeuge miteinander, aber auch mit Infrastruktur kommunizieren können.

[0006] Obwohl die meisten Vorrichtungen in einem Haushalt stationär sind, wird es als ein Nachteil wahrgenommen, wenn zur Verbindung dieser Geräte eine Verdrahtung bereitgestellt werden muss. In Szenarios mit Transportbezug, einschließlich Industry 4.0, sind die Vorrichtungen typischerweise mobil. Typischerweise werden alle der vorstehenden Szenarien als Internet-of-Things (Internet der Dinge) mit der Abkürzung IoT zusammengefasst.

[0007] Um Kommunikation zu ermöglichen, muss die Kommunikation drahtlos sein. Wie die Bezeichnung schon nahelegt, sind IoT-Vorrichtungen typischerweise mit einem öffentlichen Netzwerk verbunden. Weil Informationen in diesen Einrichtungen sensibel sein können, muss die Kommunikation sicher und zuverlässig sein. Dementsprechend muss Sicherheit tief in das Design eines drahtlosen Kommunikationssystems integriert sein, insbesondere auf der physikalischen Ebene. Solche Anforderungen führen zu zusätzlichem Aufwand bei den Nutzlastdaten.

[0008] Der größte Teil der Nutzlastdaten, die in diesen Szenarios von einer Entität an eine andere gesendet werden, ist eher klein, z.B. um 128 Bit. Diese Art von Kommunikation ist auch als Machine Type Communication (MTC) bekannt.

[0009] Kommunikationstechnologien nach dem Stand der Technik, wie etwa LTE oder WiFi, konzentrieren sich auf Übertragungen großer Dateien, z.B. Videostreaming, was effizient große Pakete nutzt. Infolgedessen besteht viel Kommunikationsaufwand für kurze Pakete, z.B. Steuerinformationen, was viel Bandbreite verschwendet. Typischerweise übersteigt der Aufwand in IoT-Szenarios in diesen Kommunikationsschemas (bei weitem) die Nutzlast.

[0010] Darüber hinaus machen viele Anwendungen, z.B. autonomes Fahren oder 14.0, eine extrem hohe Kommunikationssystemzuverlässigkeit erforderlich. Dieses Erfordernis wird häufig als fünf 9er oder 10^{-9} bezeichnet. Werden solche Zuverlässigkeitsanforderungen z.B. für 14.0 Anwendungen nicht geliefert, resultiert dies in gestoppten Produktionslinien. Im Fall des autonomen Fahrens kann dies zu fatalen Unfällen führen.

[0011] Ein Kommunikationssystem für IoT-Anwendungen muss die erforderliche Zuverlässigkeit bereitstellen oder es kann für die angedachte Anwendung nicht eingesetzt werden.

[0012] Von dieser Ausgangssituation ausgehend, ist es ein Ziel der Erfindung, Verfahren und Vorrichtungen bereitzustellen, die es ermöglichen, Aufwand zu reduzieren ohne gleichzeitig Zuverlässigkeit und Sicherheit zu kompromittieren.

Kurzdarstellung der Erfindung

[0013] Das Ziel wird durch die Verfahren nach Ansprüchen 1 bzw. die Entitäten nach Ansprüchen 2 und 3 erreicht. Weitere vorteilhafte Ausführungsformen sind Gegenstand der der Beschreibung und der beigefügten Figuren.

Figurenliste

[0014] Im Folgenden wird sich auf die Figuren bezogen. Darin zeigt

Fig. 1 ein schematisches Datenverarbeitungsschema nach dem Stand der Technik,

Fig. 2 ein schematisches Datenverarbeitungsschema gemäß den Ausführungsformen der Erfindung, und

Fig. 3 ein schematisches Flussdiagramm der Verfahrensschritte in unterschiedlichen Entitäten gemäß Ausführungsformen der Erfindung.

Ausführliche Beschreibung

[0015] Die vorliegende Offenbarung beschreibt bevorzugte Ausführungsformen unter Bezugnahme auf die Figuren, in denen gleiche Referenzzeichen die gleichen oder ähnliche Elemente repräsentieren.

[0016] Bezugnahmen in dieser Spezifikation auf „eine Ausführungsform“ oder in ähnlicher Sprache bedeuten, dass ein/e bestimmte/s Merkmal, Struktur oder Eigenschaft, die in Verbindung mit der Ausführungsform beschrieben wird, in mindestens einer Ausführungsform der vorliegenden Erfindung enthalten ist. Somit kann sich die Formulierung „in einer Ausführungsform“ und ähnliche Sprache in dieser Spezifikation stets auf die gleiche Ausführungsform beziehen, muss dies aber nicht.

[0017] Die beschriebenen Merkmale, Strukturen oder Charakteristika der Erfindung können auf jedwede geeignete Weise in einer oder mehreren Ausführungsformen kombiniert werden. In der Beschreibung werden zahlreiche spezifische Einzelheiten angeführt, um ein genaues Verständnis der Ausführungsformen der Erfindung zu ermöglichen. Das heißt, sofern nur als Alternative angegeben, kann ein Merkmal einer Ausführungsform auch in einer anderen Ausführungsform verwendet werden.

[0018] Auch wenn in manchen Fällen bestimmte Merkmale in Bezug auf eine einzelne Entität beschrieben werden, dient solch eine Beschreibung darüber hinaus nur zu veranschaulichenden Zwecken und tatsächliche Implementierungen der Erfindung können auch eine oder mehrere dieser Entitäten umfassen. Das heißt, Verwendung des Singulars schließt auch plurale Entitäten mit ein, sofern nicht anders angegeben.

[0019] Nun wird eine beispielhafte Ausführungsform unter Bezugnahme auf die Figur beschrieben.

[0020] In **Fig. 1** wird eine typische Verarbeitung in einem Kommunikationssystem nach dem Stand der Technik gezeigt, wie etwa ein Kommunikationssystem auf LTE-Basis.

[0021] Dort sind die Anforderungen an Sicherheit und Zuverlässigkeit durch unterschiedliche Domänen mit einer unabhängigen Verarbeitung verkörpert.

[0022] In der Sicherheitsdomäne sind die zwei Schlüsselziele Datenvertraulichkeit und - authentifizierung. Datenpaketinhalte werden durch Verschlüsselung vertraulich gehalten. Ansonsten können diese Informationen Produktionsdetails an nicht autorisierte Dritte durchsickern lassen.

[0023] Verschlüsselung nach dem Stand der Technik kann durch den Advanced Encryption Standard (AES) Standard ermöglicht werden. Authentifizierung verifiziert den Ursprung empfangener Pakete, um autorisierte von nicht autorisierten Daten zu unterscheiden. Dies wird häufig mit einem Message Authentication Code (MAC)zum Verifizieren der Integrität eines empfangenen Pakets ermöglicht. Die bekanntesten Optionen hierfür sind Keyed-hash Message Authentication Code (HMAC) und Cipher-based Message Authentication Code (CMAC). Das Schlüsselkonzept ist es, eine kryptographische Prüfsumme (Aufwand) der Nutzlast zur Nachrichtauthentifizierung hinzuzufügen.

[0024] In der Zuverlässigkeitsdomäne liegt der Fokus auf korrektem Paketempfang. In dieser Domäne sind viele verschiedene Weiterleitungsfehlerkanalkodierungskonzepte verfügbar. Die Integrität empfangener Pakete kann über Cyclic Redundancy Check (CRC) Kodierung mit einem hohen Sicherheitsniveau verifiziert werden. Ein CRC fügt jedem Paket eine Prüfsumme (Aufwand) zur Verifikation hinzu. Übertragungen sind für Fehler anfällig, somit stellt Forward Error Correction (FEC) Fähigkeiten zur Korrektur von Fehlern beim Empfänger bereit.

[0025] Wie bereits erwähnt, wird Paketaufwand bei kurzen Paketen, die sich häufig in M2M-Kommunikation beobachten lassen, zu einem ausgeprägten Problem.

[0026] Bei einem ausführlicheren Verständnis lässt sich feststellen, dass sowohl CRC als auch MAC jedem Paket eine Prüfsumme zur Integritätsverifikation hinzufügen. Es besteht insofern ein kleinerer Unterschied, als dass die MAC-Prüfsumme zusätzliche Funktionalität unterstützt, nämlich Authentifizierung. Grund dafür ist der gemeinsame Ansatz, dass jeder Aspekt innerhalb seiner eigenen Domäne behandelt wird und unabhängige Resultate bereitstellen sollte.

[0027] Den Erfindern ist jedoch aufgefallen, dass in dem Fall, dass man von der geschichteten Ansicht unabhängiger Zwecke abweichen würde, man Verarbeitung einer Prüfsumme vermeiden kann. Die Erfinder schlagen daher, wie in **Fig. 2** gezeigt, vor, nur die MAC-Prüfsumme zu verwenden, während man die Notwendigkeit eine CRC zu berechnen vermeidet. Daher kann man Aufwand reduzieren.

[0028] Die Erfindung schlägt daher ein Verfahren für eine sendende Entität in einer Netzwerkumgebung

vor. Das Verfahren umfasst einen Schritt des Empfangens **200** von Nutzlastinformationen für einen spezifischen Empfänger. Der Sender fügt im Schritt **300** einen Nachrichtauthentifizierungscode basierend auf einen im Voraus bekannten Schlüssel des Empfängers hinzu, um dadurch eine zu kodierende Information zu bilden. Dann wird die Information im Schritt **400** kodiert und danach im Schritt **500** zu dem Empfänger übertragen.

[0029] In Ausführungsformen der Erfindung ist das Kodieren **400** ein polares Kodieren oder ein Turbokodieren. Es ist zu beachten, dass mehrere Implementierungen existieren könnten, die es erlauben, eine Dekodierung mit einem Authentifizierungscode zu kombinieren, nämlich die Kombination eines Listendecoders und eines polaren Codes. Dies ist jedoch nicht einschränkend. Andere Codes, wie etwa Turbocodes, können ähnliche Eigenschaften bereitstellen. Somit kann das Kodieren auf dieser beabsichtigten Nutzung beruhen.

[0030] Um die hohen Zuverlässigkeitsanforderungen zu erfüllen, kann man ferner bestimmte Codes für FEC einführen. Ein Beispiel ist die Verwendung polaren Codes für FEC. Es ist bekannt, dass polare Codes eine hohe Fehlerkorrekturleistung für kurze Pakete bereitstellen. Für Einzelheiten hierzu, siehe z.B. E. Arikan, „Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels“, IEEE Transactions on Information Theory, (2009).

[0031] Für den Sender kann man polare Codes mit MAC für Aufwandreduzierung kombinieren.

[0032] Auf der empfangenden Seite schlägt die Erfindung ein Verfahren für eine empfangende Entität in einer Netzwerkumgebung vor. Das Verfahren umfasst einen Schritt des Empfangens **600** einer kodierten Information, die von dem Sender im Schritt **500** übertragen wurde. Die kodierten Informationen werden dann im Schritt **700** dekodiert, um dadurch dekodierte Informationen bereitzustellen. Danach kann man im Schritt **800** bestimmen, ob die dekodierten Informationen basierend auf einem im Voraus bekanntem Schlüssel des Empfängers authentifiziert werden können, und falls die Authentifizierung gegeben ist, werden die dekodierten Informationen oder Teile davon zur weiteren Verarbeitung weitergeleitet.

[0033] In einer Ausführungsform des empfangenden Verfahrens wird ein Nachrichtauthentifizierungscode zum Verifizieren korrekter Dekodierung oder zum Rückführen von Informationen an das Dekodierungsverfahren für erweiterte Dekodierung verwendet.

[0034] Es ist zu beachten, dass mehrere Implementierungen existieren könnten, die es erlauben, eine Dekodierung mit einem Authentifizierungscode zu kombinieren, nämlich die Kombination eines Listendecoders und eines polaren Codes. Dies ist jedoch nicht einschränkend. Andere Codes, wie etwa Turbocodes, können ähnliche Eigenschaften bereitstellen.

[0035] In einer Ausführungsform des empfangenden Verfahrens basiert das Dekodieren **700** beispielsweise derart auf einer Kandidatenliste, dass Kandidaten der Dekodierung der Bestimmung unterliegen, bis ein erster Kandidat authentifiziert wird oder das Ende der Liste von Kandidaten erschöpft ist.

[0036] Auf der Empfängerseite kann dann in Ausführungsformen der Erfindung ein Decodierer, wie der Arikan Successive Cancellation SC Decoder, verwendet werden, um ein einzelnes Informationswort zu produzieren, das durch eine Prüfsumme mit der vorgeschlagenen MAC-Prüfsumme verifiziert werden kann.

[0037] Ausgereiftere Decoder können über weitere Verwendung dieser Prüfsumme verfügen.

[0038] Beispiele für solche fortgeschrttenen Decoder finden sich in „List Decoding of Polar Codes“, I. Tal und A. Vardy, in IEEE Transactions on Information Theory, (2015), „Low-Complexity Soft-Output Decoding of Polar Codes“, U. U. Fayyaz und J. R. Barry, in IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, 32 (2014) und „Dynamic-SCFlip Decoding of Polar codes“, L. Chandesris, V. Savin und D. Declercq in IEEE Global Communications Conference (GLOBECOM), 2016.

[0039] Alle polaren Decoder nach dem Stand der Technik verwenden eine CRC-Prüfsumme, um empfangene Codewörter korrekt zu identifizieren. Wir schlagen stattdessen vor, eine MAC-Prüfsumme zu verwenden.

[0040] Diese Informationen können dann als ein frühes Stopp-Kriterium für solch einen Decoder verwendet werden oder um sich für das richtige Codewort unter vielen zu entscheiden.

[0041] Auf jeden Fall führt das resultierende System die Sicherheits- und die Zuverlässigkeitsdomäne zusammen. Es ist in Hinsicht auf Aufwand effizienter, weil der durch eine CRC-Prüfsumme verursachte Aufwand eliminiert wird.

[0042] Die Erfindung kann in jeder Art von Netzwerkumgebung verwendet werden, insbesondere in einer drahtlosen Netzwerkumgebung. Darüber hinaus kann die Erfindung in einer Mobilnetzwerksystemumgebung von besonderer Relevanz sein, wie etwa einem Public Land Mobile Netzwerk, z.B. einem Netzwerk der 2., 3., 4., 5. oder 6. Generation.

[0043] Die Netzwerkumgebung kann insbesondere eine Internet-der-Dinge-Umgebung sein.

[0044] Wie in **Fig. 3** gezeigt, kann der im Voraus bekannte Schlüssel in Richtung des Senders bereitgestellt werden, beispielsweise über einen Steuerkanal. Es kann auch andere Mittel zum Bereitstellen des im Voraus bekannten Schlüssels geben. Der im Voraus bekannte Schlüssel kann beispielsweise durch einen spezialisierten Datenbankdienst innerhalb des Netzwerks bereitgestellt werden und/oder ein im Voraus bekannter Schlüssel kann im Voraus festgelegt werden.

[0045] Die (polare) Kodierung kann in Ausführungsformen der Erfindung insbesondere FEC-Eigenschaften bereitstellen.

[0046] Darüber hinaus schlägt die Erfindung eine sendende Entität bzw. eine empfangene Entität bereit, die dafür ausgelegt sind, jedwedes der vorstehend aufgeführten Verfahren durchzuführen.

[0047] Die Erfindung weicht von dem üblichen Ansatz ab und erlaubt Integration von Sicherheits- und Zuverlässigkeitsaspekten, anstatt sie als separate Entitäten zu behandeln. Das resultierende System ist effizienter, weil Aufwand reduziert werden kann, während es eine ähnliche oder gleiche Korrekturleistung wie derzeit eingesetzte Systeme bereitstellt.

[0048] Somit erlaubt die Erfindung Aufwandreduzierung, was von großer Bedeutung für kurze M2M-Paketübertragungen ist, z.B. für 128-Bit-Pakete mit einer typischen CRC 32-Bit-Prüfsumme. Dies resultiert in einer Aufwandsreduzierung um etwa 25%.

[0049] Die Erfindung erlaubt die Aufrechterhaltung von FEC-Leistung.

[0050] Verwendung polarer Codes erlaubt es, Empfängerkomplexität zu reduzieren, insbesondere in Verbindung mit einer Prüfsumme.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

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

Zitierte Nicht-Patentliteratur

- „List Decoding of Polar Codes", I. Tal und A. Vardy, in IEEE Transactions on Information Theory, (2015) [0038]
- „Low-Complexity Soft-Output Decoding of Polar Codes", U. U. Fayyaz und J. R. Barry, in IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, 32 (2014) [0038]
- „Dynamic-SCFlip Decoding of Polar codes", L. Chandesris, V. Savin und D. Declercq in IEEE Global Communications Conference (GLOBECOM), 2016 [0038]

Patentansprüche

1. Verfahren für ein System aufweisend eine sendende Entität und eine empfangende Entität in einer Netzwerkumgebung, wobei das Verfahren für eine sendende Entität in einer Netzwerkumgebung, die Schritte aufweist:
• Empfangen (200) von Nutzlastinformationen für einen spezifischen Empfänger,
• Hinzufügen (300) eines Nachrichtauthentifizierungscodes basierend auf einem im Voraus bekannten Schlüssel des Empfängers, um dadurch eine zu kodierende Information zu bilden,
• Kodieren (400) der zu kodierenden Information,
• Senden (500) der kodierten Information in Richtung des Empfängers. und das Verfahren für eine empfangende Entität in einer Netzwerkumgebung, die Schritte aufweist:
• Empfangen (600) einer kodierten Information,
• Dekodieren (700) der kodierten Information in eine dekodierte Information,
• Bestimmen (800), ob die dekodierte Information basierend auf einem im Voraus bekanntem Schlüssel des Empfängers authentifiziert werden kann, und falls die Authentifizierung gegeben ist, Weiterleiten der dekodierten Information oder von Teilen davon zur weiteren Verarbeitung, wobei ein Nachrichtauthentifizierungscode zum Verifizieren korrekter Dekodierung oder zum Rückführen von Informationen an das Dekodierungsverfahren für erweiterte Dekodierung verwendet wird,
• wobei das Dekodieren (700) beispielsweise derart auf einer Kandidatenliste basiert, dass Kandidaten der Dekodierung der Bestimmung unterliegen bis ein erster Kandidat authentifiziert wird oder das Ende der Liste von Kandidaten erschöpft ist,
• wobei das Kodieren (400, 700) ein polares Kodieren oder ein Turbokodieren ist,
• wobei die Netzwerkumgebung eine drahtlose Netzwerkumgebung eine Internet-der-Dinge-Umgebung in einer eine Mobilnetzwerksystemumgebung ist,
• wobei der im Voraus bekannte Schlüssel über einen Steuerkanal bereitgestellt wird oder im Voraus festgelegter ist,
• wobei Kodieren FEC-Eigenschaften bereitstellt,
• wobei Dekodieren auf einem Arikan Successive Cancellation Decoder basiert.

2. Sendende Entität, die dafür ausgelegt ist, ein Verfahren nach Anspruch 1 durchzuführen.

3. Empfangende Entität, die dafür ausgelegt ist, ein Verfahren nach Anspruch 1 durchzuführen.

Es folgen 2 Seiten Zeichnungen

Anhängende Zeichnungen

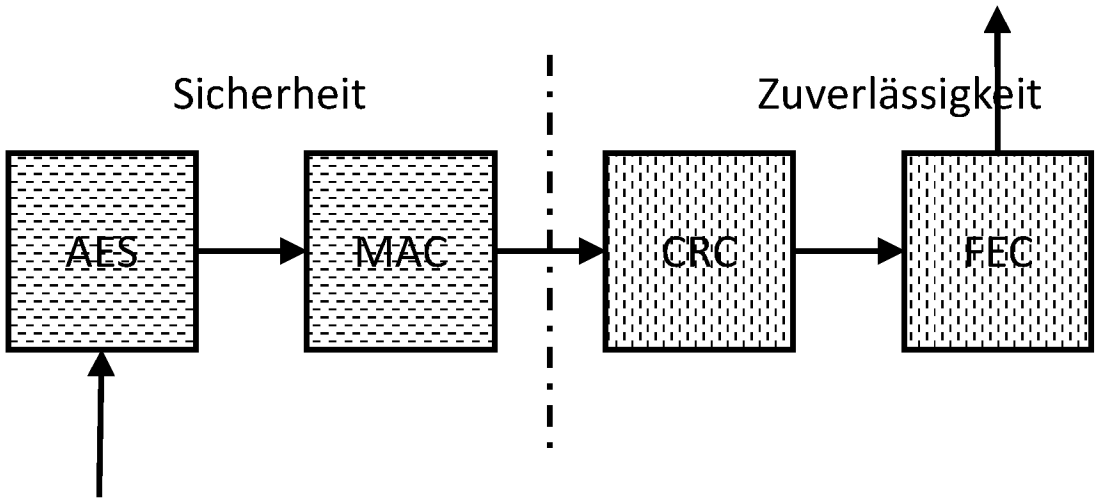


Fig. 1 – Stand der Technik

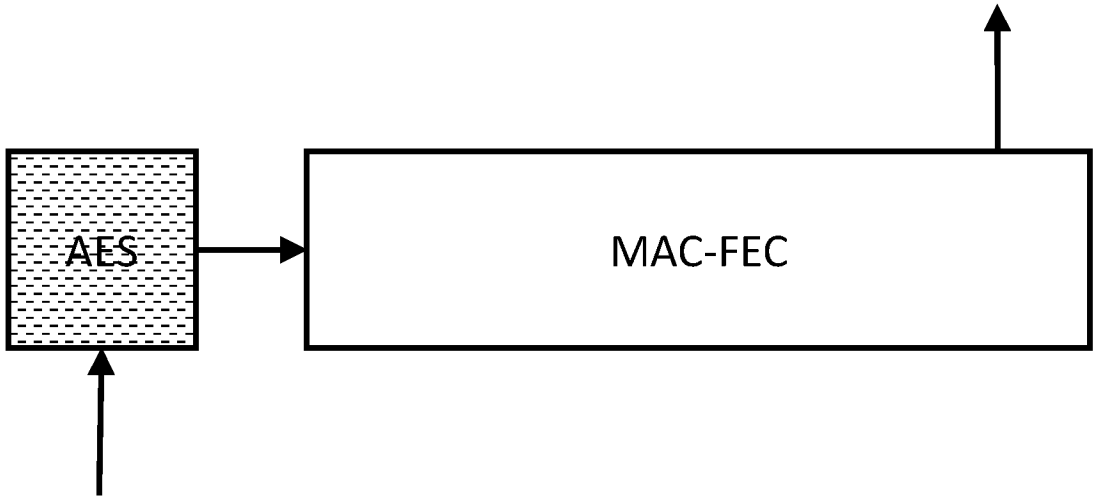


Fig. 2

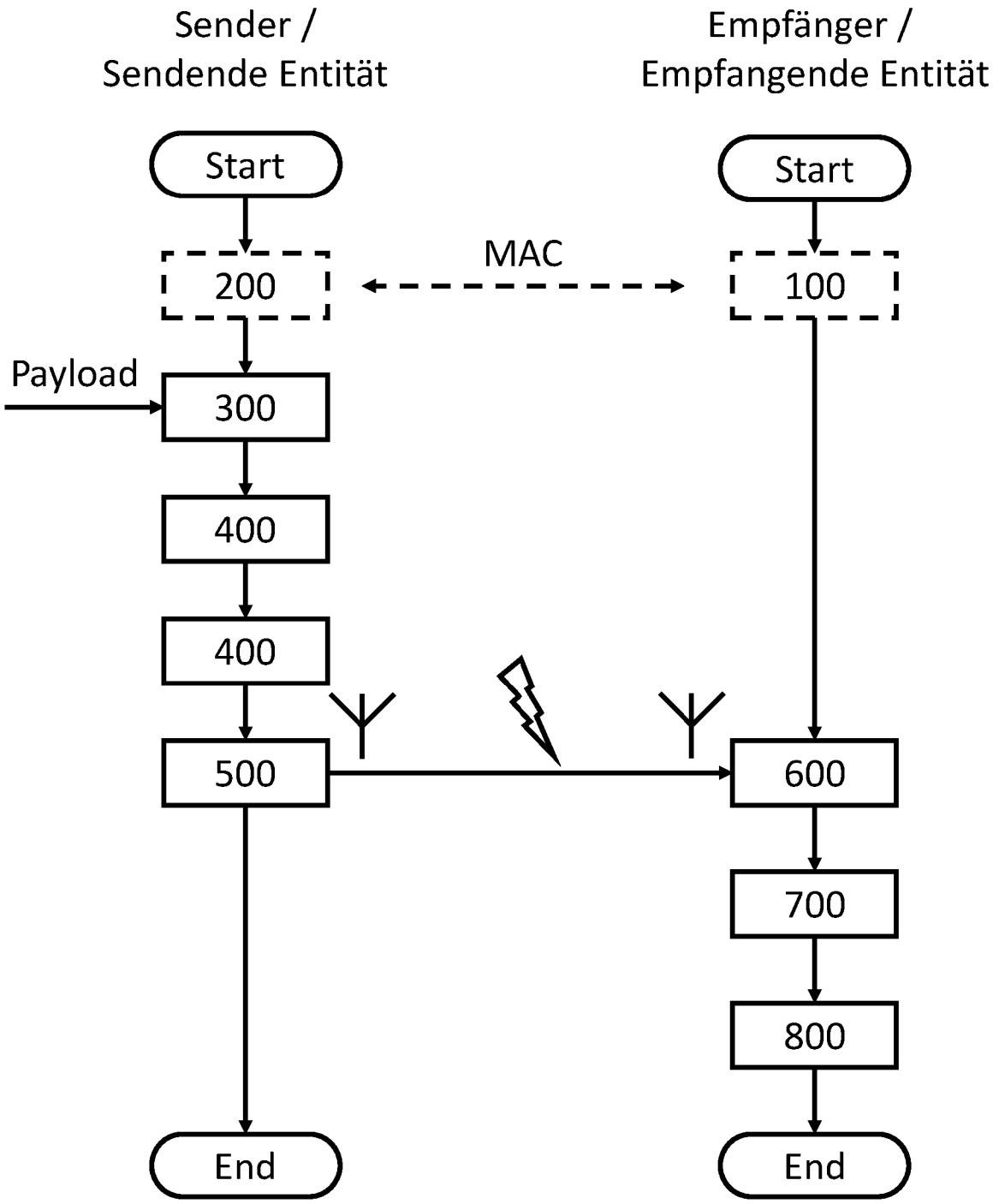


Fig. 3

