(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 601 18 259 T2** 2006.11.30

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 209 844 B1**
(21) Deutsches Aktenzeichen: **601 18 259.6**
(96) Europäisches Aktenzeichen: **01 000 597.3**
(96) Europäischer Anmeldetag: **07.11.2001**
(97) Erstveröffentlichung durch das EPA: **29.05.2002**
(97) Veröffentlichungstag
der Patenterteilung beim EPA: **29.03.2006**
(47) Veröffentlichungstag im Patentblatt: **30.11.2006**

(51) Int Cl.[8]: ***H04L 9/12*** (2006.01)

(30) Unionspriorität:
20002607 28.11.2000 FI

(84) Benannte Vertragsstaaten:
AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE, TR

(73) Patentinhaber:
EADS Secure Networks Oy, Helsinki, FI

(74) Vertreter:
Eisenführ, Speiser & Partner, 80335 München

(72) Erfinder:
Relander, Rasmus, 00150 Helsinki, FI; Stenberg, Timo, 01600 Vantaa, FI

(54) Bezeichnung: **Erhaltung der Ende-zu-Ende-Synchronisation einer Fernmeldeverbindung**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

HINTERGRUND DER ERFINDUNG

[0001] Die Erfindung betrifft ein Verfahren und eine Vorrichtung zum Aufrechterhalten bzw. Beibehalten einer Ende-zu-Ende-Synchronisation auf einer Telekommunikationsverbindung.

[0002] In Telekommunikationssystemen, wie beispielsweise einem öffentlichen Netzwerk, ist es sehr wichtig, dass kein elektronisches Mithören des Verkehrs möglich ist. Die Luftschnittstelle wird typischerweise verschlüsselt, selbst wenn der Funkverkehr überwacht wird, kann ein Außenstehender diesen nicht entschlüsseln. In einer Infrastruktur ist der Verkehr jedoch nicht notwendigerweise verschlüsselt, sodass der Verkehr, wie beispielsweise Sprache, unter Verwendung des Codec des betroffenen Systems entschlüsselt werden kann. Selbst wenn, ein Außenstehender im Prinzip nicht den Sprachfluss innerhalb der Infrastruktur belauschen kann, stellt dies ein mögliches Sicherheitsrisiko für sehr anspruchsvolle Anwender dar. Daher wurde eine Lösung entwickelt, in der Sprache mit einer Ende-zu-Ende-Verschlüsselung verschlüsselt werden kann. Ein Beispiel eines Systems, das eine Ende-zu-Ende-Verschlüsselung ermöglicht, stellt das TETRA (Terrestrial Trunked Radio System) dar. Das Dokument Sarmarkoon M.I. et al: „Encrypted video over TETRA", IEE Seminar on TETRA Market and Technology Developments (Ref. No. 9000/007), London, UK 2000, Seiten 1 bis 5, offenbart ein TETRA-System, welches eine Ende-zu-Ende-Verschlüsselung verwendet.

[0003] Die grundlegende Idee einer Ende-zu-Ende-Verschlüsselung besteht darin, dass ein Netzwerkanwender, beispielsweise eine Behörde, Verkehr verschlüsseln und entschlüsseln kann, unabhängig von und ohne Rücksicht auf das verwendete Übertragungsnetzwerk, beispielsweise in einer Endgeräteausstattung.

[0004] Im TETRA-System beispielsweise, wenn eine Ende-zu-Ende-Verschlüsselung zur Anwendung kommt, codiert der Sender zuerst ein 60-ms-Sprachsample unter Verwendung eines TETRA-Codec, wobei so ein unverschlüsseltes bzw. Klartext-Sample erzeugt wird. Das übertragende Endgerät erzeugt ein verschlüsseltes Sample, wobei ein bestimmtes Schlüsselstromsegment verwendet wird. Das verschlüsselte Muster wird dann an das Netzwerk übertragen. Der Empfänger verschlüsselt das verschlüsselte Sample durch Verwendung desselben Schlüsselstromsegments, wobei er so wieder ein unverschlüsseltes Sample enthält.

[0005] Um ein Brechen der Verschlüsselung zu verhindern, wird das Schlüsselstromsegment fortlaufend gewechselt, was bedeutet, dass jeder Rahmen, der ein 60-ms-Sprachsample enthält, mit seinem eigenen Schlüsselstromsegment verschlüsselt wird. Beide Verschlüsselungs-Stromgeneratoren müssen sich daher darauf einigen, welches Schlüsselstromsegment für jeden Rahmen verwendet wird. Diese Aufgabe gehört zur Synchronisationssteuerung. Für die Aufgabe werden Synchronisationsvektoren verwendet, die zwischen den Endgeräten mittels eines In-Band-Signals übertragen werden.

[0006] Die Verschlüsselungs-Schlüsselstromgeneratoren erzeugen einen Schlüsselstrom basierend auf einem bestimmten Schlüssel und einem Initialisierungsvektor. Die Schlüssel werden an jedes Endgerät verteilt, welches an dem verschlüsselten Anruf teilnimmt. Dies bildet einen Teil der Einstellungen der Endgeräteausstattungs. Ein neues Schlüsselstromsegment wird daher einmal alle 60-ms erzeugt. Nach jedem Rahmen wird der Initialisierungsvektor gewechselt. Die einfachste Alternative besteht darin, diesen um 1 zu erhöhen, aber jeder Verschlüsselungsalgorithmus umfasst sein eigenes Inkrementierungsverfahren, welches noch komplexer sein kann, um das Brechen des Schlüssels zu verhindern.

[0007] Die Synchronisationssteuerung ist dafür verantwortlich sicherzustellen, dass beide Enden den verwendeten Initialisierungsvektor kennen, mit dem jeder Rahmen verschlüsselt ist. Um dem Verschlüsseler und dem Entschlüsseler zu ermöglichen, sich auf den Wert des Initialisierungsvektors zu einigen, wird ein Synchronisationsvektor am Beginn jedes Sprachelements gesendet. Sobald ein Gruppenanruf betroffen ist, muss auch ein Beitreten zu dem Anruf während eines Sprachelements möglich sein. Aus diesem Grund wird der Synchronisationsvektor, z.B. 1 bis 4-mal pro Sekunde gesendet. Zusätzlich zu dem Initialisierungsvektor umfasst der Synchronisationsvektor beispielsweise eine Schlüsselkennung und eine CRC-Fehlerprüfung, um die Endgeräteausstattung in die Lage zu versetzen, die Integrität des Synchronisationsvektor zu überprüfen. Der Empfänger zählt so die Anzahl der übertragenen Rahmen nach dem Synchronisationsvektor und basierend auf dem letzten empfangenen Initialisierungsvektor und der Anzahl der Rahmen erzeugt der Schlüsselstromgenerator einen neuen Initialisierungsvektor.

[0008] Ein Datenübertragungsnetzwerk kann ein oder mehrere paketvermittelte Verbindungen umfassen, wie beispielsweise IP (Internet Protokoll)-Verbindungen, in denen Daten unter der Verwendung beispielsweise von Sprache über IP (bzw. Voice over IP, VoIP) übertragen werden. Ein Standardprotokoll zum Übertragen von Echtzeitdaten, wie beispielsweise Sprache oder Videobildern, in einem IP-Netzwerk ist beispielsweise das RTP (Echtzeitprotokoll bzw. Real Time Protocol). Das IP-Netzwerk verursacht typischerweise eine variierende Verzögerung bei der Übertragung der Pakete. Für die Sprachverständlich-

keit beispielsweise sind Schwankungen in der Verzögerung am schädlichsten. Um das zu kompensieren, speichert das Empfangsende der RTP-Übertragung ankommende Pakete in einem Jitter-Zwischenspeicher bzw. Jitter Buffer und reproduziert diese mit einer bestimmten Reproduktionszeit bzw. Wiederherstellungszeit. Ein Paket, das vor der Reproduktionszeit ankommt, nimmt an der Rekonstruktion des ursprünglichen Signals teil, wohingegen ein Paket, das nach der Reproduktionszeit ankommt, unbenutzt bleibt und verworfen wird.

[0009] Einerseits erfordert eine Echtzeitanwendung bzw. Applikation eine so kurz wie mögliche Ende-zu-Ende-Verzögerung und die Reproduktionsverzögerung sollte daher reduziert werden. Andererseits ermöglicht eine lange Reproduktionsverzögerung eine lange Empfangszeit für die Pakete und so können mehr Pakete angenommen werden. Folglich sollte der Wert der Reproduktionsverzögerung kontinuierlich entsprechend den Netzwerkbedingungen angepasst werden. Die meisten RTP-Algorithmen umfassen eine Einrichtung, die die Reproduktionsverzögerung automatisch entsprechend den Netzwerkbedingungen anpasst, um die Sprachqualitität zu verbessern. Um die Reproduktionsverzögerung um beispielsweise 60 ms nach vorne zu verschieben, erzeugt der IP-Übergang bzw. IP-Gateway ein Ersatzpaket von 60 ms. Mit anderen Worten es wird ein Extrarahmen zum Rahmenfluss, der übertragen wird, hinzugefügt. Um die Reproduktionsverzögerung rückwärts zu verschieben, wird wenigstens ein Rahmen entfernt.

[0010] Ein Problem mit der oben beschriebenen Anordnung besteht darin, dass, wenn eine synchronisierte Ende-zu-Ende-Verschlüsselungscodierung verwendet wird und ein Extrarahmen zum Rahmenfluss hinzugefügt wird, dies dazu führt, dass der Rahmenzähler am empfangenen Ende in Bezug auf die ankommenden Rahmen einen Rahmen voraus ist und daher das Schlüsselstromsegment des empfangenen Endes nicht länger dem des übertragenden Endes entspricht. Folglich, falls ein Rahmen aus dem Rahmenfluss entfernt wird, wird der Rahmenzähler am empfangenden Ende um einen Rahmen in Beziehung auf die ankommenden Rahmen verzögert und das Schlüsselstromsegment entspricht nicht mehr dem des übertragenden Endes.

[0011] Das Verschieben der Reproduktionsverzögerung während eines Sprachelements beispielsweise verursacht den Verlust der Ende-zu-Ende-Synchronisation und die verschlüsselte Sprache kann nicht länger entschlüsselt werden. Dies setzt sich fort bis das übertragende Ende einen neuen Synchronisationsvektor sendet, um das empfangende Ende zu synchronisieren. Dies kann in Semi-Duplex-Anrufen vermieden werden, beispielsweise durch Verändern der Reproduktionsverzögerung, nur nach Sprachelementen. Falls die Sprachelemente lang sind, kann die Möglichkeit, die Reproduktionsverzögerung zu verändern, nachteilig selten auftreten und daher kann die Sprachqualität bis zum Ende des gesamten Sprachelements dürftig sein, da die Reproduktionsverzögerung nicht früher geändert werden kann. Darüber hinaus kann die Reproduktionsverzögerung beispielsweise in Duplex-Anrufen, bei denen es keine Sprachelemente gibt und das Endgerät kontinuierlich überträgt, während des gesamten Anrufs, wenn der Verlust der Synchronisation vermieden werden soll, überhaupt nicht geändert werden.

KURZE BESCHREIBUNG DER ERFINDUNG

[0012] Es ist daher eine Aufgabe der Erfindung, ein Verfahren und eine Ausstattung bereitzustellen, welche das Verfahren, das es ermöglicht, die obigen Probleme zu lösen, umsetzt. Die Aufgabe der Erfindung wird gelöst durch ein Verfahren und ein System, das durch die Angaben in den unabhängigen Ansprüchen 1 und 6 charakterisiert ist. Die bevorzugten Ausführungsbeispiele der Erfindung sind in den abhängigen Ansprüchen offenbart.

[0013] Die zugrundeliegende Idee besteht darin, dass, falls die Reproduktionsverzögerung während einer Datenübertragung verändert wird, wie beispielsweise ein Sprachelement oder ein Anruf, die Zeit der Änderung derart ausgewählt wird, dass der Rahmen, der der nächste nach der Änderung sein wird, einen Synchronisationsvektor umfasst, wodurch das empfangende Ende unmittelbar nach der Änderung synchronisiert wird und es so keine Lücken in der Entschlüsselung der verschlüsselten Daten und dadurch in der Decodierung geben wird.

[0014] Ein Vorteil des Verfahrens und des Systems der Erfindung besteht darin, dass es ermöglicht, die Reproduktionsverzögerung zu verändern auch während einer Datenübertragung, ohne dass dadurch die Decodierung der verschlüsselten Daten gestört wird.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

[0015] Im Folgenden wird die Erfindung in größerem Detail in Verbindung mit den bevorzugten Ausführungsbeispielen und unter Bezugnahme auf die begleitenden Zeichnungen beschrieben, in denen:

[0016] Fig. 1 ein Blockdiagramm ist, welches die Struktur eines TETRA-Systems veranschaulicht;

[0017] Fig. 2 ein Blockdiagramm ist, welches die Funktion der Ende-zu-Ende-Verschlüsselung veranschaulicht;

[0018] Fig. 3 die Berechnung eines Initialisierungsvektors veranschaulicht, die durch den Empfänger ausgeführt wird;

[0019] Fig. 4 ein Diagramm ist, welches den Aufbau eines RTP-Pakets veranschaulicht;

[0020] Fig. 5 die Funktion eines RTP-Algorithmus veranschaulicht;

[0021] Fig. 6 ein Diagramm ist, welches die Ankunftswahrscheinlichkeit von RTP-Paketen als Funktion der Übertragungszeit veranschaulicht;

[0022] Fig. 7A ein Diagramm ist, welches die Reduzierung der Übertragungsverzögerung veranschaulicht; und

[0023] Fig. 7B ein Diagramm ist, welches die Erhöhung der Übertragungsverzögerung veranschaulicht.

DETAILLIERTE BESCHREIBUNG DER ERFINDUNG

[0024] Im Folgenden wird die Erfindung im Wege eines Beispiels unter Bezugnahme auf ein TETRA-System beschrieben. Jedoch ist nicht beabsichtigt, die Erfindung auf ein bestimmtes Telekommunikationssystem oder Datenübertragungsprotokoll zu beschränken. Die Anwendungen der Erfindung auf andere Systeme werden für den Fachmann offensichtlich sein.

[0025] Fig. 1 zeigt ein Beispiel für einen Aufbau eines TETRA-Systems. Obgleich die Netzwerkelemente, auf die in der Figur und der folgenden Beschreibung Bezug genommen wird, solche des TETRA-Systems sind, beschränkt dies keinenfalls die Anwendung der Erfindung auf andere Telekommunikationssysteme. Es ist anzumerken, dass die Figur nur solche Elemente zeigt, die für das Verständnis der Erfindung relevant sind, und die Struktur des Systems von dem offenbarten abweichen kann, ohne dass das irgendeine Relevanz für die grundlegende Idee der Erfindung hat. Es ist auch anzumerken, dass ein aktuelles mobiles Kommunikationssystem eine beliebige Anzahl von jedem Element umfassen kann. Mobilstationen MS kommunizieren mit TETRA-Basisstationen TBS über einen Funkweg. Die Mobilstationen MS können auch einen direkten Modus verwenden, um miteinander direkt zu kommunizieren, ohne die Basisstationen TBS zu verwenden. Jede Basisstation TBS ist mit einer Verbindungsleitung an eine der digitalen Vermittlungen für TETRA (BTX) des Festnetzwerks verbunden. Die TETRA-Vermittlungen DXT besitzen eine feste Verbindung zu anderen Vermittlungen und zu einem TETRA-Vermittlungsknoten DXTc (digitale zentrale Vermittlung für TETRA bzw. Digital Central Exchange for TETRA, nicht gezeigt), welche eine Vermittlung ist, die mit der andere Vermittlungen DXT und/oder Vermittlungskonteo DXTc verbunden sind, um alternative Verkehrsrouten bzw. Verkehrswege bereitzustellen. Externe Verbindungsschnittstellen, falls vorhanden, zu dem öffentlichen leitungsvermittelten Telefonnetz (bzw. Public Switch Telephone Network, PSTN), dem digitalen Netzwerk mit integrierten Diensten (bzw. integrated services digital network ISDN), einer privaten automatischen Zweigvermittlung PABX und zu einem paketvermittelten Datennetzwerk PDN können beispielsweise in einer oder mehreren Vermittlungen DXT vorhanden sein. Von den obigen Schnittstellen zeigt die Figur eine Verbindung zu dem paketvermittelten Datennetzwerk PDN über einen Netzwerkübergang bzw. Gateway GW. Der Gateway GW ist verantwortlich für das Konvertieren leitungsvermittelte Daten, die von der Vermittlung DXT kommen, in paketvermittelte Daten, die von dem Paketdatennetzwerk PDN geroutet wurden, und umgekehrt. Dies ermöglicht einer Endgeräteausstattung TE, die mit dem Paketdatennetzwerk PDN verbunden ist, mit dem TETRA-System zu kommunizieren. Der Gateway GW kann ein separates Netzwerkelement oder ein Teil der Vermittlung DXT beispielsweise sein. Weiter zeigt die Figur ein Abfertigungssystem (bzw. Dispatcher System) DS, das mit der Vermittlung DXT verbunden ist, wobei das System aus einer Abfertiger-Stationssteuerung DSC und einer Abfertigungsarbeitsstation DWS, die damit verbunden ist, besteht. Die Verwaltung des Abfertigungssystems steuert die Anrufe und andere Funktion der Mobilstationen MS über die Arbeitsstation DWS.

[0026] Fig. 2 veranschaulicht die Funktion einer Ende-zu-Ende-Verschlüsselung. Wenn eine Ende-zu-Ende-Verschlüsselung verwendet wird, verschlüsselt ein Sender **20** zuerst ein 60 ms Sprach-Sample, wobei ein TETRA-Codec verwendet wird, um ein unverschlüsseltes Sample (P) zu erzeugen. Die Mobilstation erzeugt ein Schlüselstromsegment KSS, das die Länge P besitzt, an einem Verschlüsselungsschlüsselstromgenerator **21**. Ein verschlüsseltes Sample (C) wird erhalten durch Ausführen einer binären XOR-Operation in Block **22**:

C = PxorKSS

[0027] Das verschlüsselte Sample wird anschließend an ein Übertragungsnetzwerk **29** übertragen. Ein Empfänger **30** führt die gleiche XOR-Operation in Block **28** durch Verwendung desgleichen Schlüsselstromsegments aus, um das unverschlüsselte Sample P zu erzeugen:

P = CxorKSS

[0028] Um das Brechen der Verschlüsselung zu verhindern, wird das Schlüsselstromsegment KSS fortlaufend gewechselt und so wird jeder Rahmen mit einem separaten Schlüsselstromsegment verschlüsselt. Beide Verschlüsselungsschlüsselstromgeneratoren **21** und **27** müssen daher in dem Schlüsselstromsegment, das für jeden Rahmen zu verwenden ist, übereinstimmen. Diese Aufgabe gehört zur Syn-

chronisationssteuerung **23** und **26**. Für diesen Zweck werden Synchronisationsvektoren verwendet, die zwischen der Endgeräteausstattung mittels eines In-Band-Signals übertragen wurden.

[0029] Der Verschlüsselungsschlüsselstromgenerator (EKSG) **21** und **27** erzeugt ein Schlüsselstromsegment (KSS) basierend auf einem Schiffrierschlüssel (CK) und einem Initialisierungsvektor (IV). Ein neues Schlüsselstromsegment wird einmal alle 60 ms erzeugt.

KSS = EKSG (CK, IV)

[0030] Nach jedem Rahmen wird der Initialisierungsvektor gewechselt. Der einfachste Weg, dies auszuführen, besteht darin, den Vektor um 1 zu inkrementieren, jedoch umfasst jeder Verschlüsselungsalgorithmus sein eigenes Inkrementierungsverfahren, das sogar noch komplexer sein kann, um das Brechen der Verschlüsselung zu verhindern.

[0031] Die Synchronisationssteuerung **23** und **26** ist verantwortlich dafür sicherzustellen, dass beide Enden **20** und **30** den Initialisierungsvektor, der für die Verschlüsselung jedes Rahmens verwendet wurde, kennen. Um den Verschlüsseler **20** und dem Entschlüsseler **30** zu ermöglichen, in dem Wert des Initialisierungsvektors übereinzustimmen, wird ein Synchronisationsvektor (SV) zu Beginn eines jeden Sprachelements zu übertragen. Wenn ein Gruppenanruf betroffen ist, muss ein sich dem Anruf anschließen möglich sein, selbst während eines Sprachelements. Für diesen Zweck wird der Synchronisationsvektor fortlaufend ungefähr 1 bis 4 mal pro Sekunde übertragen. Zusätzlich zum Initialisierungsvektor umfasst der Synchronisiervektor eine Schlüsselkennung und eine CRC-Fehlerprüfung beispielsweise, die es der Endgeräteausstattung ermögliche, die Integrität des Synchronisierungsvektors zu überprüfen.

[0032] Der Empfänger **30** zählt so die Anzahl der Rahmen (n), die nach dem Synchronisierungsvektor übertragen worden sind. Der Schlüsselstromgenerator **27** des Empfängers **30** erzeugt einen neuen Initialisierungsvektor IV basierend auf dem letzten empfangenen Initialisierungsvektor und der Anzahl der Rahmen. Das Zählen des Initialisierungsvektors IV, welches durch den Empfänger ausgeführt wird, ist in Fig. 3 veranschaulicht, welche die Rahmenabfolge, die übertragen werden soll, zeigt. Rahmen 1, 6, 12 und 13 der Abfolge umfassen einen Synchronisierungsvektor SV, der über die Anzahl der Initialisierungsvektoren IV informiert.

[0033] Die Enden **20** und **30** sollten beide darin übereinstimmen, wie ein Anruf zu verschlüsseln ist. An beiden Enden vorgesehene Synchronisierungs-Steuerungseinheiten **23** und **26** kommunizieren miteinander mittels U-gestohlener Sprachblöcke. Die übertragende Endgeräteausstattung verwendet einen oder mehrere Sprachblöcke innerhalb des Rahmens für seine eigene Zwecke. Dies findet in Block **24** statt. Dies wird der empfangenden Endgeräteausstattung angezeigt durch geeignetes Setzen von drei ersten Steuerbits innerhalb des Rahmens. Die Infrastruktur **29** versteht so, dass die betroffenen Daten Endgeräte-zu-Endgerät-Daten sind und daher überträgt es die Datentransparent, ohne diese zu verändern. Zusätzlich umfasst die empfangene Endgeräteausstattung, dass der betroffene Sprachblock keine Sprachdaten umfasst und schickt sie daher nicht zum Codec, sondern verarbeitet sie entsprechend, d.h. Synchronisierungs-Steuerungsdaten werden zur Synchronisierungs-Steuerung **26** in Block **25** gefiltert und die empfangende Steuerung erzeugt einen Ersatzton, um die gestohlene Sprache zu ersetzen. Das Stehlen eines Sprachblocks löscht 30 ms Sprache. Dies würde eine Unterbrechung in der Sprache verursachen, welche die Sprachqualität beeinträchtigen und es das Verständnis erschweren würde. Um dies zu vermeiden, umfasst der TETRA-Codec einen Ersatzmechanismus. In Realität empfindet der Anwender das Fehlen von Sprache nicht als unangenehm, vorausgesetzt, das Sprachblöcke nicht mehr als 4-mal pro Sekunde gestohlen werden. Jedes Endgerät, das an einem verschlüsselten Anruf teilnimmt, empfängt einen Chifrierschlüssel CK; dies wurde in den Einstellungen der Endgeräteausstattung festgelegt.

[0034] Das in der Fig. 1 gezeigte paketvermittelte Datennetzwerk PDN kann beispielsweise das Internet sein, welches TCP/IP-Protokolle verwendet. TCP/IP ist die Bezeichnung für eine Familie von Datenübertragungsprotokollen, die innerhalb eines Lokalbereichsnetzwerks bzw. Local Area Network oder zwischen diesen verwendet werden. Die Protokolle sind IP (Internet Protokoll), TCP (Übertragungssteuerungsprotokoll bzw. Transmission Controll Protocol) und UTP (Anwenderdatagrammprotokoll bzw. User Datagram Protocol). Die Familie umfasst auch andere Protokolle für bestimmte Dienste, wie beispielsweise Dateiübertragung, E-Mail, Fernanwendung, etc.

[0035] TCP/IP-Protokolle werden in Schichten unterteilt: Datenverbindungsschicht (bzw. Data Link Layer), Netzwerkschicht (bzw. Network Layer), Transportschicht (bzw. Transport Layer) und Anwendungsschicht (bzw. Application Layer). Die Datenverbindungsschicht ist verantwortlich für den physikalischen Zugriff des Endgeräts auf das Netzwerk. Es steht hauptsächlich mit der Netzwerkschnittstellenkarte und dem Treiber (bzw. Driver) in Beziehung. Die Netzwerkschicht wird auch oft als die Internetschicht oder IP-Schicht bezeichnet. Diese Schicht ist beispielsweise verantwortlich für die Übertragung von Paketen innerhalb des Netzwerkes und für deren Routing von einem Gerät zu einem anderen basierend auf einer IP-Adresse. Die Netzwerkschicht wird

durch das IP in der TCP/IP-Protokollfamilie bereitgestellt. Die Transportschicht stellt einen Datenflussdienst zwischen zwei Endgeräten für die Anwendungsschicht bereit und leitet den Fluss zu der richtigen Anwendung in dem Endgerät. Es gibt zwei Übertragungsprotokolle im Internet-Protokoll: TCP und UDP. Eine andere Aufgabe der Transportschicht besteht darin, die Pakete an die richtige Anwendung basierend auf Port-Nummern zu leiten. TCP stellt einen verlässlichen Datenfluss von einem Endgerät zu einem anderen bereit. TCP unterteilt bzw. splittet die Daten in Pakete von geeigneter Größe, bestätigt empfangene Pakete und steuert, dass übertragene Pakete als empfangen am anderen Ende bestätigt werden. TCP ist verantwortlich für eine zuverlässige Ende-zu-Ende-Übertragung, d. h. die Anwendung muss sich nicht darum kümmern. Andererseits ist UDP ein viel einfacheres Protokoll. UDP ist nicht verantwortlich für die Ankunft von Daten und falls dies erforderlich ist, ist dafür die Anwendungsschicht verantwortlich. Die Anwendungsschicht ist verantwortlich für die Datenverarbeitung jeder Anwendung.

[0036] RPT ist ein Standard-Internet-Protokoll für die Übertragung von Echtzeitdaten, wie beispielsweise Sprache und Videobildern. Es kann verwendet werden für Ondemand-Media-Dienste (bzw. Media-Dienste auf Anforderung) oder interaktive Dienste wie beispielsweise IP-Anrufe. RTP setzt sich zusammen aus einem Media-Teil und einen Steuer-Teil, der letztere wird RTCP (Echtzeitsteuerungsprotokoll bzw. Real Time Controll Protocol) genannt. Der RTP-Media-Teil stellt eine Unterstützung für Echtzeitanwendungen einschließlich Zeitunterstützung, Verlustentdeckung, Sicherheitsunterstützung und Inhaltserkennung bereit. RTCP ermöglicht Echtzeitkonferenzen innerhalb Gruppen unterschiedlicher Größe und Bewertungen der Ende-zu-Ende-Dienstqualität. Es unterstützt auch die Synchronisierung von einer Vielzahl von Media-Flüssen. RTP wurde entworfen, um unabhängig vom Übertragungsnetzwerk zu sein, obwohl im Internet-Netzwerk RTP normalerweise IP-UDP anwendet. Das RTP-Protokoll umfasst verschiedene Merkmale die Echtzeit-Ende-zu-Ende-Datenübertragung ermöglichen. An jedem Ende sendet eine Audio-Anwendung regulär kleine Audio-Daten-Sample von beispielsweise 30 ms. Jedes Sample wird mit einem RTP-Header bzw. RTP-Kopf versehen. Der RTP-Kopf und die Daten werden dann in UDP und IP-Pakete gepackt.

[0037] Der RTP-Kopf kennzeichnet den Inhalt eines Pakets. Der Wert dieses Felds zeigt das Codierungsverfahren (PCM, ADPCM, LPC, etc.), welches in der RTP-Paketnutzlast zu verwenden ist. Über das Internet sowie über andere Paketnetzwerke übertragene Pakete können in einer zufälligen Reihenfolge ankommen, um eine variierende Zeit verzögert sein oder sogar vollständig verschwinden. Um dies zu verhindern, wird jedem Paket in einem bestimmten Fluss eine Sequenznummer und ein Zeitstempel, entsprechend dem ein empfangener Fluss wieder angeordnet wird, um dem ursprünglichen zu entsprechen, zugeordnet. Die Sequenznummer wird um eins für jedes Paket erhöht. Die Sequenznummern ermöglichen den Empfänger ein fehlendes Paket zu erfassen und außerdem Paketverlust zu bewerten.

[0038] Der Zeitstempel ist eine 32-Bit-Nummer, die den Zeitpunkt anzeigt, wenn das Sampling beginnt. Er wird berechnet, unter Verwendung eines Takts, der sich gleichmäßig und linear entlang der Zeit erhöht. Die Taktfrequenz muss ausgewählt werden, um für den Inhalt geeignet zu sein, schnell genug zum Berechnen des Jitter und um Synchronisierung zu ermöglichen. Beispielsweise wenn ein PCM-A-Law-Codierungsverfahren verwendet wird, beträgt die Taktfrequenz 8000 Hz. Wenn RTP-Pakete mit 240 Byts übertragen werden, was 240 PCM-Samples entspricht, wird der Zeitstempel um 240 für jedes Paket erhöht. Die Länge eines RTP-Kopfes ist 3 bis 18 words lang (a 32-bits pro Word). Fig. 4 veranschaulicht das Format eines RTP-Pakets. Die Felder haben folgende Bedeutung: V = Version, d. h. die verwendete RTP-Version, im Moment 2. Füller = das Paket umfasst Füller-Bits, wobei das letzte Bit deren Anzahl anzeigt. Erweiterung = genau eine Kopf-Erweiterung nach dem Paket. PM = die Anzahl der Dienstquellen, welche anzeigt, wie viele Quellen die Information für das Paket erzeugt haben. Eine Markierung kann verwendet werden zum Anzeigen wesentlicher Ereignisse, wie beispielsweise Rahmengrenzen. HAT = Nutzlast-Typ, der den Media-Typ, der in der Nutzlast enthalten ist, anzeigt. Die laufende Nummer wird um eins für jedes übertragene Paket erhöht. Sie unterstützt beim Erfassen von Paketverlust und Störung. Ihr Anfangswert ist zufällig. Der Zeitstempel zeigt den Augenblick des Samplings des ersten Byts an. Er wird verwendet zur Synchronisierung und zur Jitter-Berechnung. Sein anfänglicher Wert ist zufällig. SSRC = eine zufällig ausgewählte Synchronisierungsquellen-Kennung, die den Verbindungspunkt der Quelle oder des ursprünglichen Senders anzeigt, falls es nicht nur eine Quelle gibt. CSRC-Liste ist eine Liste von Quellen, die in dem Paket enthalten sind.

[0039] Das Internet verursacht eine schwankende Verzögerung in der Übertragung von Audio-Paketen, was sich am schädlichsten auf die Sprachverständlichkeit auswirkt. Um dies zu kompensieren, speichert das empfangene Ende des RTP ankommende Pakete in einen Jitter-Zwischenspeicher bzw. Jitter-Buffer und reproduziert diese zu einer bestimmten Reproduktionszeit. Ein Paket, das vor der Reproduktionszeit ankommt, nimmt an der Rekonstruierung des ursprünglichen Signals teil, wo hingegen ein Paket, das nach der Reproduktionszeit ankommt, unverwendet bleibt und verworfen wird.

[0040] Fig. 5 veranschaulicht die Funktion eines RTP-Algorythmus. In der Figur werden verwendet der Buchstabe t um die Übertragungszeit des Pakets, der Buchstabe a die Zeit des Empfang und p die Zeit der Reproduktion zu kennzeichnen. Überschriften kennzeichnen die Paketnummer und Unterschriften die Nummer des Sprachelements. In dem K-ten-Sprachelement kommen die Pakete an den empfangenen Enden nach einer schwankenden Übertragungszeit an. Der RTP-Algorythmus reproduziert anschließend zum korrekten Zeitpunkt. Im (K + 1)-ten Sprachelement wird die Anordnung der Pakete 1 und 2 gewechselt; Paket 4 kommt nach der Reproduktionszeit an und wird daher verworfen. Der RTP-Algorythmus stellt die korrekte Reihenfolge der Pakete wieder her, reproduziert diese zum korrekten Zeitpunkt und zeigt fehlende oder verzögerte Pakete beispielsweise für Korrekturoperationen an. Die Reproduktionsverzögerung ist die Zeit t (Reproduktionsverzögerung) = t (Reproduktion) – t (Übertragung). Der RTP-Algorhytmus stellt sicher, dass die Reproduktionsverzögerung für die gesamte Dauer des Sprachelements konstant bleibt.

[0041] Die Verzögerung des IP-Paket durch das Netzwerk t = t (Eingabe) – t (Ausgabe) besteht aus zwei Elementen. L ist eine feste Verzögerung, die von der Übertragungszeit und der durchschnittlichen Warteschlangenzeit abhängt und J ist eine schwankende Verzögerung, die von einer schwankenden Warteschlangenzeit innerhalb des IP-Netzwerk abhängt und Jitter verursacht. An dem empfangenen Ende des IP-Netzwerks gibt es einen Jitter-Buffer, der die Pakete in seinem Speicher speichert, falls die Übertragungszeit t < t (Reproduktionsverzögerung) ist. Die Bestimmung der Reproduktionsverzögerung ist ein Kompromiss. Einerseits erfordert eine Echtzeitanwendung eine so kurz wie mögliche Ende-zu-Ende-Verzögerung und daher sollte die Reproduktionsverögerung reduziert werden. Andererseits ermöglicht eine lange Reproduktionsverzögerung eine lange Zeit für die Ankunft der Pakete und dadurch können mehr Pakete angenommen werden. Der Wert der Reproduktionsverzögerung sollte daher laufend entsprechend den Netzwerkbedingungen angepasst werden. Dies ist in Fig. 6 veranschaulicht. Ein Paket mit einer Übertragungszeit t < L + J kann angenommen werden, wohin gegen ein Paket mit einer Übertragungszeit t > L + J verworfen werden muss. Durch Erhöhung von J ist es daher möglich, die Anzahl der angenommenen Pakete zu erhöhen. Die Reproduktionsverzögerung kann angepasst werden beispielsweise durch Starten mit einem kleinen Wert und anschließend Erhöhen dieses Wertes gleichmäßig, bis der Anteil der verzögerten Pakete unter einer bestimmten Grenze, beispielsweise 1 %, bleibt.

[0042] Die meisten RTP-Algorythmen schließen ein Dienstmerkmal ein, welches die Reproduktionsverzögerung automatisch entsprechend dem Netzwerkbedingungen anpasst, um die Sprachqualität zu verbessern. Die Reproduktionsverzögerung kann beispielsweise 60 ms durch Erzeugen eines Ersatz-Sprachpaket von 60 ms am RTP-Empfang nach vorne verschoben werden bevor der Sprachfluss sich fortsetzt. Mit anderen Worten ein zusätzlicher Rahmen wird zum Sprachfluss hinzugefügt. Wenn die Reproduktionsverzögerung um 60 ms nach hinten verschoben wird, wird ein ganzer Sprachrahmen beim RTP-Empfang entfernt.

[0043] In Fig. 1 findet RTP-Übertragung zwischen dem Netzwerkübergang bzw. Gateway GW und der Endgeräteausstattung TE so über das Paketnetzwerk PDN statt. Der Gateway GW ist verantwortlich für die Konvertierung von leitungsvermittelter Sprache (oder anderen Daten), die von der Vermittlung DXT über eine PCM-Verbindung kommen, in IP-Sprachpakete und umgekehrt. In der TETRA-Infrastruktur werden Sprachdaten in Rahmen übertragen und so würde ein natürliches RTP-Paket einen Rahmen mit Sprachdaten umfassen. Ein RTP-Paket würde so 60 ms Sprache enthalten und direkt dem Inhalt eines Sprachrahmens entsprechen. Eine andere Option besteht darin, ein RTP-Paket, das nur einen halben Rahmen mit Sprachdaten (30 ms) enthält, zu verwenden. Verglichen mit einem vollständigen Rahmenpaket weist ein Halb-Rahmen-Paket die folgenden Eigenschaften auf: 1) Wenn der Gateway Halb-Rahmen-Pakete empfängt, muss er auf die Ankunft von 2 Paketen warten, bevor die Übertragung eines ISI-Rahmens begonnen wird. Die Steuer-Bits (BFIC- oder U-gestohlen) von beiden Sprachblöcken finden sich nämlich am Beginn des Rahmens und der Gateway muss diese basierend auf dem Typ der Halb-Rahmen-Pakete bestimmen. 2) Falls ein RTP-Paket verloren wird, werden nur 30 ms Speichersprachen fehlen, an Stelle von 60 ms. Wenn die Sprachqualität optimiert werden soll, stellt die Paketlänge einen Kompromiss zwischen zwei Ansätzen dar. Eine extreme Alternative besteht in einem kurzen Paket, was bedeutet, dass die Anzahl der fehlenden Pakete sich umgekehrt proportional zur Paketgröße erhöht und so Störungen häufiger auftreten. Das andere Extrem besteht in einem langen Paket, was bedeutet, dass Störungen seltener auftreten, aber die Wahrscheinlichkeit des Verlierens eines ganzen Phonems sich erhöht und dadurch die Sprachverständlichkeit beeinträchtigt wird, insbesondere wenn die Paketlänge über 20 ms beträgt. Die letztere Grenze stellt nämlich die kürzeste Phonem-Länge dar. 3) Aus dem Blickwinkel der Bandweite ist jedoch ein langes Paket effizienter, da die Länge (36–40 Byts) der Köpfe (Ethernet + IP + UDP + RTP) bereits lang ist im Vergleich mit der Länge der Nutzlast (18 Byts/Sprachblock oder 36 Byts/Sprachrahmen). Es gibt zwei Verfahren zum Reduzieren des Kopfabschnitts in einem Paket. Multiplexing kann verwendet werden, zum Packen einer mehrfachen Anzahl von

Sprachkanälen in ein und dasselbe RTP-Paket, um den Kopfabschnitt zu reduzieren. Die ist höchst relevant für eine Vermittlungs-zu-Abfertigungs-Punkt Verbindung, da es ermöglicht alle Gruppenanrufe und einen einzelnen Anruf in einem Paket zu übertragen. Ein anderes Verfahren, welches für serielle Verbindungen geeignet ist, besteht in Kopfkomprimierung. Es erlaubt einen IP/UDP/RTP-Kopf deutlich zu verkürzen (2–4 Byts), so dass Bandbreite gespart wird. Für bessere Sprachqualität ist ein kurzes RTP-Paket (mit 30 ms) mehr zu bevorzugen.

[0044] Sprachblöcke können aus einem Rahmen entweder für Zwecke des Netzwerks (C-gestohlen) oder des Anwenders (U-gestohlen) gestohlen werden. Beispielsweise wenn Ende-zu-Ende-Verschlüsselung verwendet wird, stehlen mobile Stationen einen Sprachblock 1 bis 4 mal pro Sekunde zu ihren eigenen Zwecken, um den Synchronisierungsvektor wie oben beschrieben, zu übertragen.

[0045] Der RTP-Standard und viel IP-Sprachendgeräte unterstützen ACELP-Codecs, aber der RTP-Standard unterstützt nicht den TETRA-spezifischen ACELP. Sprache kann unter Verwendung eines RTP-Pakets übertragen werden, die folgenden Einstellungen vorausgesetzt: RTP-Version 2, keine Füller, keine Erweiterung, keine CRSC-Quellen, keine Markierungen bzw. Marker, Lasttyp: 8 (dasselbe wie A-Law), Zeitstempel wird um 240 Einheiten für jedes Paket erhöht. Dies entspricht dem TETRA-Sampling-Takt von 8000 Hz und der Sampling-Länge von 30 ms. Die folgenden Daten werden in der Nutzlast vorgesehen: Die drei ersten Bits zeigen an, ob ein Rahmen-Fehler-Bit (BFI) gesetzt worden ist, falls die Nutzlast Sprachen oder Daten enthält, und falls ein C- oder U-gestohlener Sprachblock betroffen ist; andere Bits des ersten Byts werden nicht verwendet; die nächsten 137 Bits umfassen die Nutzlast und entsprechen einen Sprachblock. Der Rest der Nutzlast sind Null-Bits.

[0046] Die obige Funktion des Gateway GW zwischen einer leitungsvermittelnden und einer paketvermittlenden Verbindung ist lediglich eine Implementierungsalternative, wobei Abweichungen davon nicht relevant für die grundlegende Idee der Erfindung sind.

[0047] Die in Fig. 1 gezeigte Endgeräteausstattung TE kann ein Sprachendgerät oder ein Datenendgerät sein und die Erfindung kann auf Sprachverbindungen, Videoverbindungen oder Datenverbindungen, die Echtzeitdatenübertragung erfordern, angewendet werden. Die Endgeräteausstattung TE kann beispielsweise eine Mobilstation, eine Abfertigungsarbeitsstation, eine Basisstation oder irgendein anderes Netzwerkelement sein. Die Endgeräteausstattung TE ist nicht notwendigerweise direkt mit dem Paketnetzwerk PDN verbunden, aber es kann ein zweites TETRA-Netzwerk beispielsweise der Endgeräteausstattung TE und dem Paketnetzwerk PDN geben. In diesem Fall gibt es also an dem anderen Ende der Paketverbindung PDN ein Gateway-Element. Es kann außerdem eine andere Verbindung oder eine Mehrfachanzahl von Paketverbindungen zwischen den Elementen geben. Falls die Endgeräteausstattung TE direkt mit dem Paketnetzwerk PDN, wie in Fig. 1 zeigt, verbunden ist, funktioniert sie als die andere Partei der RTP-Übertragung im Wesentlichen ähnlich zu der Funktion des Gateway GW, der oben beschrieben worden ist.

[0048] Gemäß der Erfindung wird die Reproduktionsverzögerung am empfangenen Ende GW oder TE der Paketverbindung PDN während der Datenübertragung, beispielsweise eines Sprachelements oder eines Anrufs, zu solche einem Zeitpunkt verändert, dass der als nächstes zu übertragende Rahmen eine Synchronisationsvektor enthält. Gemäß dem bevorzugten Ausführungsbeispiel wird dies durch Überwachen der ankommenden Rahmen am empfangenen Ende GW oder TE der Paketverbindung PDN und Erkennen der Synchronisierungsvektoren, die in den Rahmen enthalten sind, ausgeführt. Damit kann eine möglicherweise benötigte Veränderung in der Reproduktionsverzögerung zeitlich so geplant werden, dass sie zu einem Zeitpunkt stattfindet, an dem der nächste Rahmen, der weitergeleitet werden soll, einen Synchronisierungsvektor umfasst. Als Beispiel sei eine Situation untersucht, die in Fig. 1 gezeigt ist, in der es einen Anruf zwischen der Mobilstation MS und einer Endgeräteausstattung TE über die Paketverbindung PDN gemäß der RTP-Protokoll gibt. Die Datenübertragung gemäß RTP-Protokoll findet so zwischen dem Gateway GW und der Endgeräteausstattung TE, welche das Protokoll unterstützen, statt. Der Gateway, der das empfangende Ende auf der Paketverbindung PDN im Hinblick auf den Verkehr, der von der Endgeräteausstattung TE kommt, überwacht die Rahmen, die von der Endgeräteausstattung kommen, in seinem Empfangszwischenspeicher bzw. Empfangs-Buffer und erkennt die darin enthaltene Synchronisierungsvektoren. Wenn gemäß dem RTP-Algorhytmus ein Bedarf festgestellt wird, die Reproduktionsverzögerung zu verändern, wird die Veränderung in dem Gateway GW zu einem Zeitpunkt ausgeführt, zu dem der nächste Rahmen, der von dem Gateway GW in Richtung der Mobilstation weiterzuleiten ist, einen Synchronisierungsvektor enthält. Der Verschlüsselungsalgorythmus der Mobilstation MS wird so unmittelbar nach der Veränderung synchronisiert, selbst wenn Rahmen von der Rahmenfrequenz entfernt oder zu der Rahmenfrequenz hinzugefügt worden sind, da ein Rahmen der einen leeren Raum oder einem zusätzlichen Rahmen folgt, einen Synchronisierungsvektor umfasst. Entsprechend überwacht die Endgeräteausstattung TE, welche das empfangende Ende auf der Paketverbindung PDN für von der Mobilstation MS kommenden

Verkehr darstellt, die von dem Gateway GW kommenden Rahmen und die darin enthaltenen Synchronisierungsvektoren. Wenn gemäß dem RTP-Algorythmus ein Bedarf, die Reproduktionsverzögerung zu verändern, festgestellt wird, wird die Veränderung an der Endgeräteausstattung TE zu einem Zeitpunkt ausgeführt, nachdem der nächste Rahmen, der zur Entschlüsselung und Reproduktion weiterzuleiten ist, einen Synchronisierungsvektor umfasst, wobei die Entschlüsselung der Endgeräteausstattung TE dadurch unmittelbar nach der Änderung synchronisiert wird. Unter Bezugnahme auf das Diagramm in Fig. 2 findet die Reproduktionsverzögerungsteuerung an der Endgeräteausstattung TE damit vor dem Filterblock **25** statt. Fig. 7a veranschaulicht die Reduzierung der Reproduktionsverzögerung gemäß der Erfindung an dem empfangenden Ende GW oder TE der Paketverbindung PDN. Die Figur zeigt eine zu empfangende Rahmensequenz **73**, von der einer oder mehrere Rahmen **71** entfernt werden und eine Rahmensequenz **74** zur Weiterleitung erhalten wird. Die Rahmen **71** werden erfindungsgemäß genau vor einem Rahmen SVF, der den Synchronisierungsvektor enthält, entfernt. Entsprechend veranschaulicht Fig. 7b die erfindungsgemäße Erhöhung der Reproduktionsverzögerung an dem empfangenen Ende GW oder TE der Paketverbindung PDN. Die Figur zeigt eine zu empfangende Rahmenfrequenz **75**, zu der ein oder mehrere Rahmen **72** hinzugefügt werden und eine Rahmensequenz **76** zum Weiterleiten erhalten wird. Erfindungsgemäß werden die Rahmen **72** genau vor dem Rahmen, der den Synchronisierungsvektor SVF enthält, hinzugefügt.

[0049] Es ist für den Fachmann offensichtlich, dass ebenso wie die Technik fortschreitet, die grundlegende Idee der Erfindung auf verschiedene Weisen implementiert werden kann. Die Erfindung und Ihre Ausführungsbeispiele werden daher nicht durch die vorstehenden Beispiele beschränkt, sondern können innerhalb des Bereichs der Ansprüche variieren.

Patentansprüche

1. Verfahren zum Beibehalten einer Ende-zu-Ende-Synchronisation auf einer Telekommunikationsverbindung, auf der Daten in Rahmen im Wesentlichen in Echtzeit übertragen werden und die eine synchronisierte Ende-zu-Ende-Verschlüsselung verwendet, die durch Übertragen von Synchronisationsvektoren in den Rahmen synchronisiert wird, und wobei zumindest ein Teil der Telekommunikationsverbindung eine paketvermittelte Verbindung ist, **dadurch gekennzeichnet**, dass die Wiedergabeverzögerung der gerade übertragenen Daten erhöht werden kann durch Hinzufügen einer oder mehrerer Zusatzrahmen zu der gerade übermittelten Rahmensequenz, und verringert werden kann durch Entfernen einer oder mehrerer Rahmen aus der gerade übermittelten Rahmensequenz, wobei das Verfahren die Schritte umfasst:
Überwachen von an dem Empfangsende der paketvermittelten Verbindung ankommenden Rahmen;
Identifizieren von in den Rahmen enthaltenen Synchronisationsvektoren; und
Ändern der Wiedergabeverzögerung an dem Empfangsende der paketvermittelten Verbindung während der Datenübertragung in einem solchen Moment, dass der als nächstes nach der Änderung an dem Empfangsende der paketvermittelten Verbindung zu übermittelnde Rahmen einen Synchronisationsvektor aufweist.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die paketvermittelte Verbindung ein Internetprotokoll einsetzt.

3. Verfahren nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, dass die Telekommunikationsverbindung zu dem TETRA-System gehört.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass die Verschlüsselung durchgeführt wird unter Verwendung eines unter Verwendung eines Initialisierungsvektors erzeugten Schlüsselstromsegments.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass der Synchronisationsvektor einen Initialisierungsvektor aufweist.

6. Anordnung zum Beibehalten einer Ende-zu-Ende-Synchronisation auf einer Telekommunikationsverbindung, auf der Daten in Rahmen im Wesentlichen in Echtzeit übertragen werden und die eine synchronisierte Ende-zu-Ende-Verschlüsselung verwendet, die durch Übertragung von Synchronisationsvektoren in den Rahmen synchronisiert wird, und wobei zumindest ein Teil der Telekommunikationsverbindung eine paketvermittelte Verbindung (PDN) ist, dadurch gekennzeichnet, dass die Wiedergabeverzögerung von gerade übertragenen Daten erhöht werden kann durch Hinzufügen eines oder mehrerer Zusatzrahmen zu der gerade übermittelten Rahmensequenz, und verringert werden kann durch Entfernen eines oder mehrerer Rahmen aus der gerade übermittelten Rahmensequenz, und dass die Anordnung Wiedergabeverzögerungseinstellmittel (GW, TE) aufweist, die angeordnet sind zum Überwachen von an dem Empfangsende der paketvermittelten Verbindung (PDN) ankommenden Rahmen;
Identifizieren von in den Rahmen enthaltenen Synchronisationsvektoren; und
Ändern der Wiedergabeverzögerung an dem Empfangsende der paketvermittelten Verbindung (PDN) während der Datenübertragung in einem solchen Moment, dass der als nächstes nach der Änderung an dem Empfangsende der paketvermittelten Verbindung übermittelte Rahmen einen Synchronisationsvektor aufweist.

7. Anordnung nach Anspruch 6, dadurch gekennzeichnet, dass die paketvermittelte Verbindung ein Internetprotokoll einsetzt.

8. Anordnung nach einem der Ansprüche 6 oder 7, dadurch gekennzeichnet, dass die Telekommunikationsverbindung zu dem TETRA-System gehört.

9. Anordnung nach einem der Ansprüche 6 bis 8, dadurch gekennzeichnet, dass die Verschlüsselung durchgeführt wird unter Verwendung eines Schlüsselstromsegments, das unter Verwendung eines Initialisierungsvektors erzeugt wird.

10. Anordnung nach einem der Ansprüche 6 bis 9, dadurch gekennzeichnet, dass der Synchronisationsvektor einen Initialisierungsvektor aufweist.

Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

Fig. 1

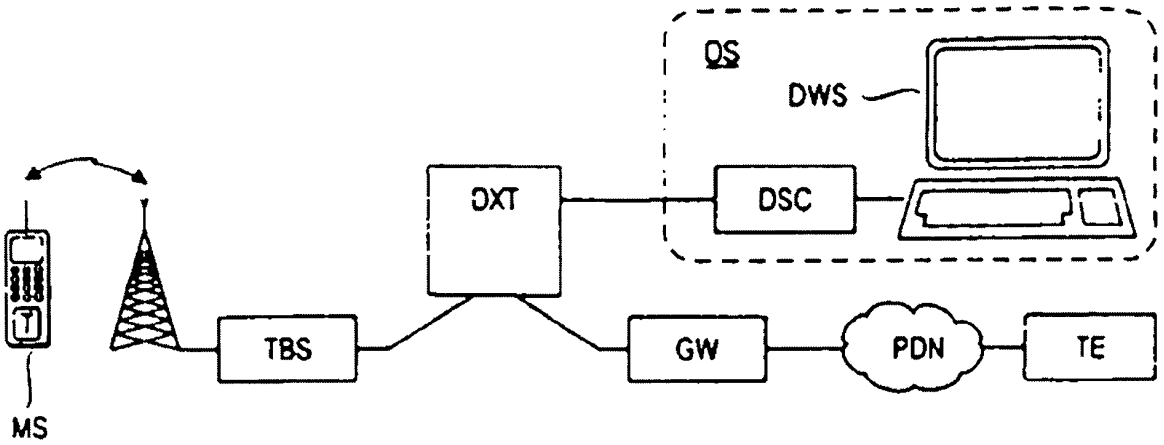

Fig. 3

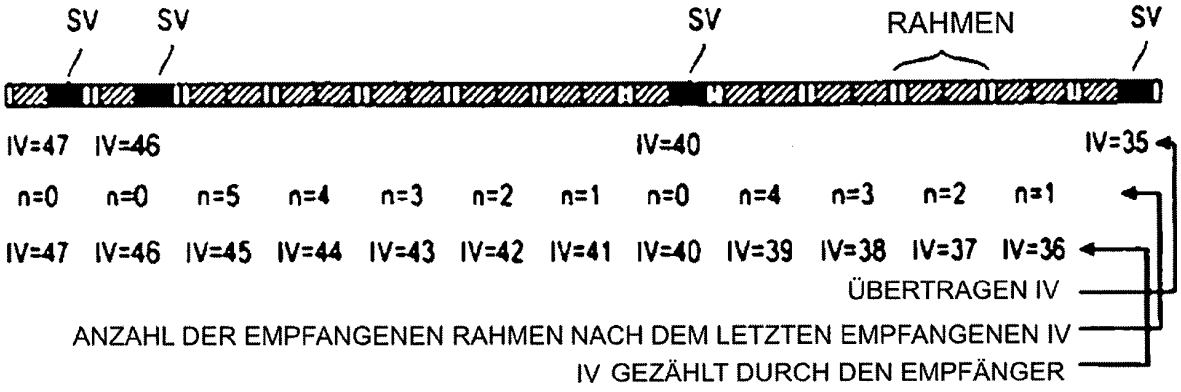

Fig. 4

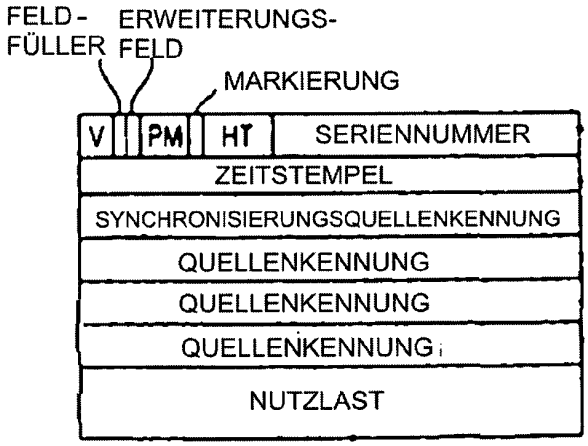

Fig. 2

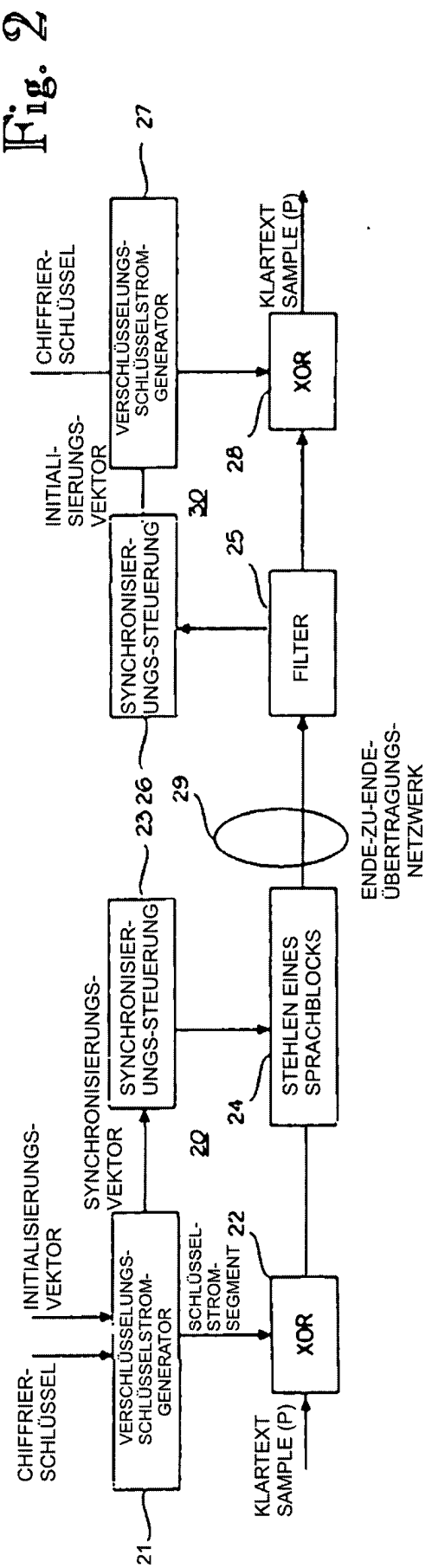
CHIFFRIER-SCHLÜSSEL
INITIALISIERUNGS-VEKTOR
VERSCHLÜSSELUNGS-SCHLÜSSELSTROM-GENERATOR
SCHLÜSSEL-STROM-SEGMENT
XOR
KLARTEXT SAMPLE (P)
SYNCHRONISIERUNGS-VEKTOR
SYNCHRONISIER-UNGS-STEUERUNG
STEHLEN EINES SPRACHBLOCKS
ENDE-ZU-ENDE-ÜBERTRAGUNGS-NETZWERK
FILTER
INITIALI-SIERUNGS-VEKTOR
VERSCHLÜSSELUNGS-SCHLÜSSELSTROM-GENERATOR
CHIFFRIER-SCHLÜSSEL
XOR
KLARTEXT SAMPLE (P)
21
22
23
24
25
26
27
28
29
30
20

Fig. 5

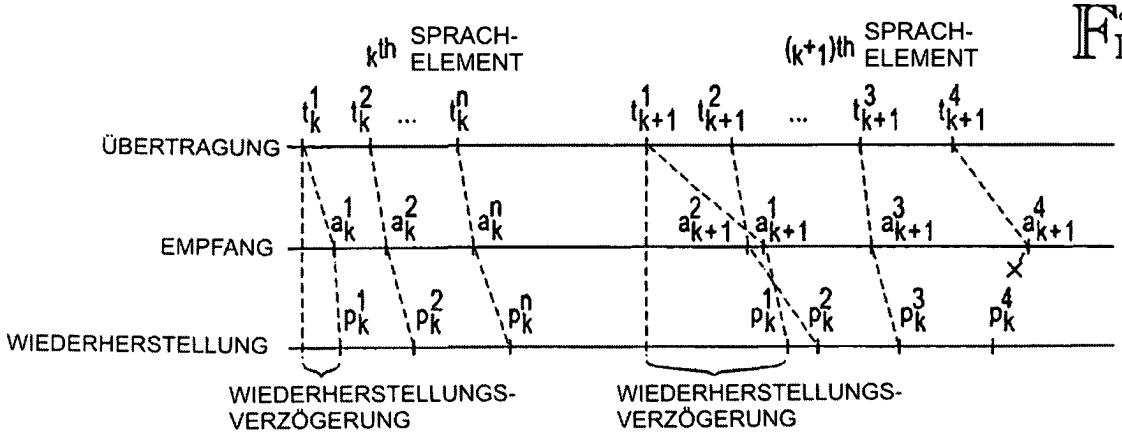

Fig. 6

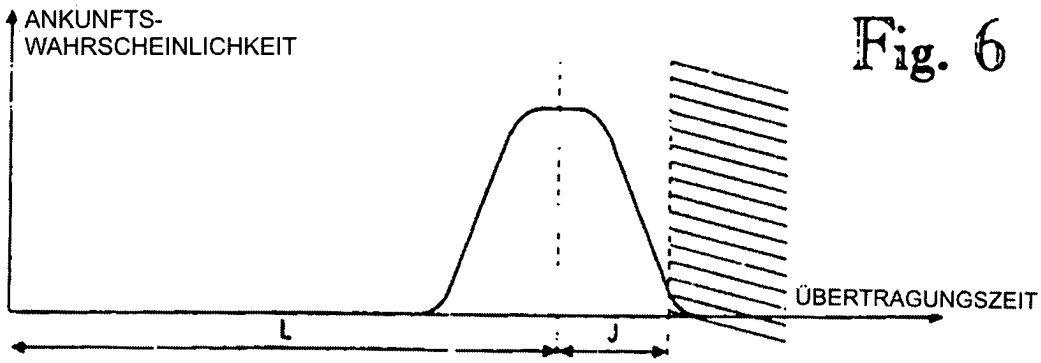

Fig. 7A

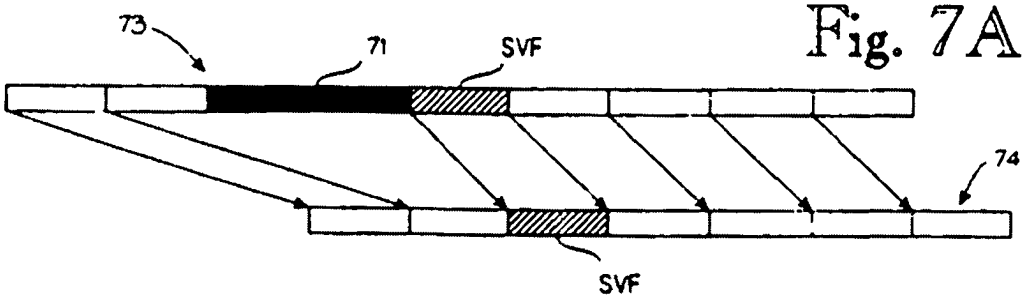

Fig. 7B