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

(10) **DE 603 07 482 T2** 2007.03.29

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 536 592 B1**
(21) Deutsches Aktenzeichen: **603 07 482.0**
(96) Europäisches Aktenzeichen: **03 292 926.7**
(96) Europäischer Anmeldetag: **26.11.2003**
(97) Erstveröffentlichung durch das EPA: **01.06.2005**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **09.08.2006**
(47) Veröffentlichungstag im Patentblatt: **29.03.2007**

(51) Int Cl.[8]: ***H04L 12/28*** (2006.01)
H04Q 7/38 (2006.01)

(73) Patentinhaber:
France Telecom, Paris, FR

(74) Vertreter:
derzeit kein Vertreter bestellt

(84) Benannte Vertragsstaaten:
AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LI, LU, MC, NL, PT, RO, SE, SI, SK, TR

(72) Erfinder:
Calmels, Benoit, 14000 Caen, FR; Maguy, Christophe, 14750 St Aubin sur Mer, FR; Trillaud, Sebastien, 35530 Servon sur Vilaine, FR

(54) Bezeichnung: **Authentifizierung zwischen einem zellularen Mobilendgerät und einem kurzreichweitigen Zugangspunkt**

Beschreibung

[0001] Die vorliegende Erfindung betrifft allgemein den Aufbau einer Verbindung zwischen einem Zugriffspunkt eines drahtlosen Netzes geringer Reichweite, von der Art Bluetooth oder Wi-Fi, und einer Mobilstation eines zellularen Funkverkehrsnetzes vom Typ GSM, die mit einem Sender-Empfänger-Modul ausgestattet ist, um mit einem Zugriffspunkts des Netzes geringer Reichweite zu kommunizieren. Sie betrifft insbesondere die Erzeugung eines Verbindungsschlüssels bei der Authentifizierung der Mobilstation und des Zugriffspunkts, um sie paarweise zu verbinden.

[0002] Bezüglich der Sicherheit insbesondere einer Bluetooth-Funkverbindung, wenn zum Beispiel ein Benutzer eine Bluetooth-Verbindung zwischen einem Laptop und einer zellularen Mobilstation herstellen möchte, gibt er einen PIN-Identifikationscode als Geheimschlüssel in die Tastaturen des Computers und der Mobilstation ein. Der Computer und die Mobilstation erstellen je einen Verbindungsschlüssel in Abhängigkeit von unter ihnen ausgetauschten Zufallszahlen, von dem Geheimschlüssel und von den Bluetooth-Adressen des Computers und der Mobilstation. Wenn zum Beispiel der PC als der Authentifikator der Verbindung betrachtet wird, erzeugt er eine Zufallszahl (challenge), die er über die Bluetooth-Funkschnittstelle an die Mobilstation überträgt. Die Mobilstation berechnet eine Antwort, die von der empfangenen Zufallszahl, vom Verbindungsschlüssel und von der Bluetooth-Adresse der Mobilstation abhängt, damit der Computer die Antwort der Mobilstation mit derjenigen vergleicht, die er selbst berechnet hat, wodurch die Mobilstation authentifiziert wird, wenn die verglichenen Antworten identisch sind.

[0003] Die paarweise Verbindung des Computers und der Mobilstation erfordert einen Geheimschlüssel (PIN-Code), um den Verbindungsschlüssel zu teilen. Der Geheimschlüssel muss lang genug und darf nicht in Wörterbüchern vorhanden sein, damit der Geheimschlüssel keinen Angriffen ausgesetzt ist, deren Ziel es ist, ihn wieder zu finden, um aus ihm den Verbindungsschlüssel und anderen kryptographischen Schlüssel abzuleiten. Solche Angriffe stellen die Authentifizierung und die Unversehrtheit der ausgetauschten Daten in Frage.

[0004] Um sich gegen diese Angriffe zu wappnen, muss der Geheimschlüssel relativ lang sein, was zu einer mühsamen und fehleranfälligen Eingabe führt, insbesondere bei der Mobilstation, deren Mensch-Maschine-Schnittstelle begrenzt ist.

[0005] Die Patentanmeldung US 2002/031228 A1 offenbart eine Zugangsvorrichtung, zum Beispiel, um eine Hotelzimmertür zu öffnen. Die Zugangsvorrichtung kann über eine Bluetooth-Verbindung mit einer Mobilstation eines zellularen Funkverkehrsnetzes verbunden sein. Die Mobilstation erfordert eine Verbindung mit einem zum Hotel gehörenden Server über das zellulare Netz oder eine Bluetooth-Verbindung. Der Server überträgt dann einen Schlüssel an die Mobilstation. Nach einer Verbindung mit der Zugangsvorrichtung sendet die Mobilstation den Schlüssel an die Zugangsvorrichtung, die den empfangenen Schlüssel mit einem in der Zugangsvorrichtung gespeicherten Schlüssel vergleicht, um ihn zu validieren und den Zugang zum Zimmer zu liefern. Es ist keine Authentifizierung der Mobilstation durch die Zugangsvorrichtung vorgesehen.

[0006] Der Artikel von Uri Blumenthal et al. "A Scheme for Authentification and Dynamic Key Exchange in Wireless Networks", Bell Labs Technical Journal 7(2), S. 37-48, 2002, beschreibt eine Kombination von Authentifizierungen für eine Mobilstation, die von einem "Haus"-Netz geringer Reichweite abhängt, von dem ein Authentifizierungsserver einen Geheimschlüssel enthält, der ebenfalls vorher in der Mobilstation gespeichert wird, wenn sie mit einem Zugriffspunkt in Verbindung steht, der mit dem Authentifizierungsserver eines anderen Netzes geringer Reichweite, "Fremd"-Netz genannt, verbunden ist. Der Server des Hausnetzes authentifiziert sowohl die Mobilstation als auch den Server des Fremdnetzes auf der Basis eines ersten "Authentifikators", der von der Mobilstation in Abhängigkeit vom Geheimschlüssel, von Zufallsnummern, die vom Server des Fremdnetzes und der Mobilstation geliefert werden, und von einem Identifikator der Mobilstation berechnet wird. Der erste Authentifikator wird an den Server des Hausnetzes über den Zugriffspunkt und den Server des Fremdnetzes übertragen. Der Server des Hausnetzes berechnet den ersten Authentifikator erneut, insbesondere in Abhängigkeit von dem gespeicherten wieder gefundenen Geheimschlüssel entsprechend dem Identifikator der Mobilstation, der vom Server des Fremdnetzes übertragen wurde.

[0007] Wenn die Mobilstation nach einer Identität der ersten übertragenen und neu berechneten Authentifikatoren, die von jedem Sitzungsschlüssel unabhängig sind, authentifiziert wird, erzeugt der Server des Hausnetzes einen zweiten "Authentifikator" in Abhängigkeit vom Geheimschlüssel, von den Zufallszahlen und von dem Identifikator der Mobilstation und berechnet einen Sitzungsschlüssel in Abhängigkeit vom Geheimschlüssel, von einer dritten Zufallszahl und vom zweiten Authentifikator. Der zweite Authentifikator wird an die Mobilstation über den Server des Fremdnetzes und den Zugriffspunkt übertragen, damit die Mobilstation den zweiten Authentifikator erneut berechnet und den Server des Hausnetzes authentifiziert, wenn die zweiten übertragenen und neu berechneten Authentifikatoren gleich sind. Nach dieser vom Sitzungsschlüssel unabhängigen zweiten Authentifizierung erzeugt die Mobilstation den Sit-

zungsschlüssel.

[0008] Alle vorhergehenden Parameter werden über die Verbindung Mobilstation – Zugriffspunkt – Server des Fremdnetzes – Server des Hausnetzes übertragen, ohne irgendeine Verbindung über das Hausnetz zwischen der Mobilstation und dem Server des Hausnetzes, was voraussetzt, vorher den Geheimschlüssel in der Mobilstation und dem Server des Hausnetzes zu speichern, um eine Sicherung der Authentifizierungen zu respektieren, wobei gleichzeitig die Authentifizierungen durch die Verwendung des gleichen Geheimschlüssels zur Erzeugung des Sitzungsschlüssels jeder Sitzung zwischen der Mobilstation und einem Zugriffspunkt geschwächt werden.

[0009] Die Patentanmeldung WO 02/07135 A1 betrifft die Aktivierung eines interaktiven Endgeräts, das ausgehend von einer Mobilstation in einem Funktelefonnetz mit einem Fernsprechnetz verbunden ist. Die Mobilstation signalisiert ihre Anwesenheit in der Nähe des Endgeräts, insbesondere durch Übertragung einer Mitteilung, die den Mobilstation-Identifikator und einen Lokalisierungsbereich-Identifikator des Funktelefonnetzes enthält, an eine Verwaltungseinrichtung, die den Benutzer der Mobilstation auffordert, sich dem am nächsten liegenden Endgerät zu nähern, in dem der Benutzer mit Hilfe eines Geheimcodes, der in einer Speicherkarte gelesen wird, oder eines biometrischen Abdrucks des Benutzers authentifiziert wird, der über das Endgerät an einen Server übertragen wird. Die Patentanmeldung WO 02/07135 A1 schlägt keine gegenseitige Authentifizierung der Mobilstation und des Endgeräts über das Funktelefonnetz vor.

[0010] Die Erfindung hat zum Ziel, den Aufbau einer Verbindung zwischen einer zellularen Mobilstation und einem Zugriffspunkt zu einem drahtlosen Netz geringer Reichweite zu sichern, ohne die Eingabe eines Geheimschlüssels (PIN-Code) zu erfordern und gleichzeitig die Verwendung eines solchen Schlüssels zu gewährleisten, der sehr lang sein kann und bei jeder Sitzung zwischen der Mobilstation und einem Zugriffspunkt erneuert wird.

[0011] Um dieses Ziel zu erreichen, ist ein vor einer Sitzung ausgeführtes Authentifizierungsverfahren zwischen einem drahtlosen Netz geringer Reichweite mit Zugriffspunkten und einer Mobilstation in einem zellularen Funkverkehrsnetz dadurch gekennzeichnet, dass es die folgenden Schritte aufweist:

– Übertragung einer Anfrage, die eine Adresse der Mobilstation und eine Adresse eines Zugriffspunkts enthält, der sich im Versorgungsgebiet der Mobilstation bezüglich des Netzes geringer Reichweite befindet, von der Mobilstation über das zellulare Netz zu einer Verwaltungseinrichtung,

– Bestimmung eines Geheimcodes durch die Verwaltungseinrichtung,

– ausgehend von der Verwaltungseinrichtung, Übertragung einer Bestätigungsmitteilung, die den Geheimcode und die aus der Anfrage entnommene Adresse des Zugriffspunkts enthält, an die Mobilstation über das zellulare Netz, und einer Verbindungsanforderungsmitteilung, die den Geheimcode und die aus der Anfrage entnommene Adresse der Mobilstation enthält, an den Zugriffspunkt,

– Anforderung einer Verbindung von der Mobilstation zu dem von der aus der Bestätigungsmitteilung entnommenen Adresse bezeichneten Zugriffspunkt, damit die Mobilstation und der Zugriffspunkt in Abhängigkeit von der Adresse des Zugriffspunkts, der Adresse der Mobilstation und vom aus der Bestätigungsmitteilung und aus der Verbindungsanforderungsmitteilung entnommenen Geheimcode einen Sitzungsschlüssel bestimmen, und

– Authentifizierung der Mobilstation durch den Zugriffspunkt in Abhängigkeit vom Sitzungsschlüssel.

[0012] Die Authentifizierung kann ausgehend vom Zugriffspunkt eine Anforderung der Bestimmung einer Antwort in Abhängigkeit vom Sitzungsschlüssel an die Mobilstation, die die Antwort über das Netz geringer Reichweite an den Zugriffspunkt überträgt, und im Zugriffspunkt eine Bestimmung einer Antwort in Abhängigkeit vom Sitzungsschlüssel und einen Vergleich der Antworten enthalten, um die Eröffnung einer Sitzung zwischen dem Zugriffspunkt und der Mobilstation zu erlauben, wenn mindestens die verglichenen Antworten gleich sind.

[0013] Vorzugsweise wird die vorhergehende Authentifizierung der Mobilstation durch den Zugriffspunkt durch eine Authentifizierung des Zugriffspunkts durch die Mobilstation in Abhängigkeit vom Sitzungsschlüssel vervollständigt, wenn der Zugriffspunkt die Mobilstation authentifiziert hat. In diesem Fall kann das Verfahren nach einer Identität der im Zugriffspunkt verglichenen Antworten eine Einladung aufweisen, die an die Mobilstation übertragen wird, damit die Mobilstation den Zugriffspunkt authentifiziert, indem sie vom Zugriffspunkt fordert, eine zweite Antwort in Abhängigkeit vom Sitzungsschlüssel zu bestimmen und die zweite Antwort über das Netz geringer Reichweite an die Mobilstation zu übertragen, indem sie eine zweite Antwort in Abhängigkeit vom Sitzungsschlüssel bestimmt, und indem sie die zweiten Antworten vergleicht, damit die Eröffnung der Sitzung erst nach einer Identität der in der Mobilstation verglichenen zweiten Antworten erlaubt wird.

[0014] In der Praxis ist es vorzuziehen, dass die Mobilstation mehrere Zugriffspunkte im Versorgungsgebiet der Mobilstation sucht, um Adressen der gefundenen Zugriffspunkte in die Anfrage einzufügen. Die

Verwaltungseinrichtung wählt dann die Adresse eines optimalen Zugriffspunkts unter den Zugriffspunktadressen aus, die aus der Anfrage gemäß einem oder mehreren vorbestimmten Kriterien entnommen werden, um die Adresse des optimalen Zugriffspunkts in die Bestätigungsmitteilung, die an die Mobilstation übertragen wird, und in die Verbindungsanforderungsmitteilung einzufügen, die an den optimalen Zugriffspunkt übertragen wird.

[0015] Gemäß einer Variante bestimmt die Verwaltungseinrichtung den Sitzungsschlüssel anstelle der Bestimmungen des Sitzungsschlüssels in der Mobilstation und im Zugriffspunkt, und fügt den bestimmten Sitzungsschlüssel anstelle des Geheimcodes in die Bestätigungsmitteilung und die Verbindungsanforderungsmitteilung ein, damit bei der Authentifizierung die zu vergleichenden Antworten insbesondere in Abhängigkeit von dem Sitzungsschlüssel bestimmt werden, der aus den vorhergehenden Mitteilungen entnommen wird.

[0016] Die Erfindung betrifft auch ein Authentifizierungssystem zwischen einem drahtlosen Netz geringer Reichweite mit Zugriffspunkten und einer Mobilstation in einem zellularen Funkverkehrsnetz, das gemäß Anspruch 14 gekennzeichnet ist.

[0017] In einer Variante kann die Verwaltungseinrichtung selbst den Sitzungsschlüssel bestimmen und ihn anstelle des Geheimcodes in die Bestätigungsmitteilung und die Verbindungsanforderungsmitteilung einfügen.

[0018] Weitere Merkmale und Vorteile der vorliegenden Erfindung gehen klarer aus der nachfolgenden Beschreibung mehrerer bevorzugter Ausführungen der Erfindung hervor, die als nicht einschränkende Beispiele zu verstehen sind und sich auf die entsprechenden beiliegenden Zeichnungen beziehen. Es zeigen:

[0019] Fig. 1 ein schematisches Blockdiagramm eines Fernsprechsystems, das eine Mobilstation in einem zellularen Funkverkehrsnetz und mindestens einen Zugriffspunkt in einem drahtlosen Netz geringer Reichweite zur Anwendung des erfindungsgemäßen Authentifizierungsverfahrens aufweist; und

[0020] Fig. 2 Hauptschritte eines Algorithmus des Authentifizierungsverfahrens zwischen der Mobilstation und dem Zugriffspunkt gemäß der Erfindung.

[0021] Das in Fig. 1 gezeigte Fernsprechsystem zur Anwendung des erfindungsgemäßen Authentifizierungsverfahrens weist hauptsächlich eine zellulare Mobilstation TM in einem zellularen Funkverkehrsnetz RC, einen oder mehrere Zugriffspunkte AP, die über ein Verteilernetz RD in einem drahtlosen Netz geringer Reichweite RFP verbunden sind, das Zugang zu einem Hochgeschwindigkeits-Paketnetz RP, wie zum Beispiel das Internet, gewährt, und eine erfindungsgemäße Verwaltungsplattform PFG auf. Zum Beispiel ist das zellulare Netz RC ein GSM-Netz, und das drahtlose Netz geringer Reichweite RFP ist ein Bluetooth-Netz.

[0022] Die Mobilstation TM weist zwei Funkschnittstellen mit dem zellularen Netz RC bzw. mit dem Netz geringer Reichweite RFP auf.

[0023] Die Zugriffspunkte AP, und in einer Variante die Mobilstationen, weisen je einen Pseudozufallsgenerator auf und verwalten je einen Authentifizierungsalgorithmus AA, um Antworten RP1, RP2 zu erzeugen, je in Abhängigkeit von einer Zufallszahl, einem Geheimcode und der Adresse der Mobilstation oder des Zugriffspunkts im Netz geringer Reichweite RFP. Ein Sitzungsschlüsselalgorithmus AS wird ebenfalls in den Zugriffspunkten und der Mobilstation ausgeführt.

[0024] Das zellulare Netz RC, zum Beispiel ein GSM-Netz, ist schematisch in Fig. 1 durch Haupteinrichtungen dargestellt, mit denen die Mobilstation TM vorübergehend verbunden ist, wie eine Basisstation BTS, eine Basisstationsteuerung BSC, ein Schalter des mobilen Diensts MSC, der einer Besucherdatei VLR zugeordnet ist, und eine Heimatdatei HLR.

[0025] Die Verwaltungsplattform PFG ist mit der Heimatdatei HLR entweder direkt, als eine mit der Heimatdatei HLR verbundene Authentifizierungszentrale (nicht dargestellt), oder als Server über ein Zwischennetz wie das Internet RP verbunden. Die Plattform PFG kann ebenfalls mit einer Kurzmitteilungszentrale SMSC (Short Message Service Center) verbunden sein, wenn Anfragen RQ an sie in Form von Kurzmitteilungen von Mobilstationen übertragen werden, und/oder kann mit einer Signalisierungsnachrichtenzentrale USSD (Unstructured Supplementary Service Data) verbunden sein, wenn Anfragen RQ an sie in Form von USSD-Mitteilungen von Mobilstationen übertragen werden. Die USSD-Mitteilungen werden während wirklicher aufgebauter Sitzungen und schneller als Kurzmitteilungen übertragen. Die Kurzmitteilungszentrale und die Signalisierungsnachrichtenzentrale werden nachfolgend unterschiedslos als "Mitteilungszentrale CM" bezeichnet. Die Plattform PFG enthält insbesondere einen Pseudozufallsgenerator, um Geheimcodes CS auf Anforderung von Mobilstationen wie der Mobilstation TM zu erzeugen. Die Geheimcodes haben erfindungsgemäß eine große Länge von typischerweise mindestens sechzehn Bytes, d.h. eine Länge von mehr als 128 Bits.

[0026] Die Plattform PFG enthält gemäß Varianten der Erfindung eine Datenbasis, die die Adressen ADAP der Zugriffspunkte AP mehrerer drahtloser Netze geringer Reichweite auflistet, zusammen mit

den geographischen Lokalisierungen der Zugriffspunkte AP bezüglich bestimmter Lokalisierungsbereiche ZL im zellularen Netz RC. Es wird daran erinnert, dass ein Lokalisierungsbereich in einem zellularen Netz mehrere Zellen versorgt, die jeweils Basisstationen BTS zugeordnet sind, und dass ein Schalter MSC einen oder mehrere Lokalisierungsbereiche verwaltet.

[0027] Wie man nachfolgend sehen wird, bildet die Plattform PFG eine Zwischen-Verwaltungseinrichtung zwischen einer Mobilstation TM und einem Zugriffspunkt AP, um ihnen eine Geheimcode CS zu übertragen, um ihre Authentifizierung durchzuführen. Gemäß weiter unten beschriebenen Varianten dient die Plattform PFG ebenfalls zur Auswahl eines optimalen Zugriffspunkts als Antwort auf eine Anfrage RQ einer Mobilstation.

[0028] In Fig. 1 ist nur ein drahtloses Netz geringer Reichweite dargestellt; es ist klar, dass die Mobilstation TM mit jedem drahtlosen Netz geringer Reichweite kommunizieren kann, insbesondere an einem öffentlichen Ort wie einem Bahnhof, einer Einkaufsgalerie, einem Flughafengebäude, einem Hotel, usw. Ein Funkzugriffspunkt AP ist zum Beispiel ein Endgerät, das mit einer Bluetooth-Funkschnittstelle, um in einem Radius von einigen zehn Metern mit Mobilstationen TM kommunizieren zu können, und mit einer Leitungsschnittstelle versehen ist, um einerseits mit anderen Zugriffspunkten AP über das Verteilernetz RD, wenn es existiert, des drahtlosen Netzes geringer Reichweite zu kommunizieren, und um andererseits aufgrund einer Verbindung des Verteilernetzes RD mit dem Internet RP den Mobilstationen Kommunikationen von Hochgeschwindigkeitspaketen anzubieten. Bei bestimmten Konfigurationen des drahtlosen Netzes geringer Reichweite ist das Verteilernetz RD ein Intranet, das direkt über xDSL-Leitungen mit dem Internet RP verbunden ist, oder aber das Verteilernetz RD fällt mit dem Internet RP zusammen, und jeder Zugriffspunkt AP ist über xDSL-Leitungen direkt mit dem Internet RP verbunden.

[0029] Wie in Fig. 2 gezeigt, weist das Authentifizierungsverfahren gemäß einer bevorzugten Ausführung der Erfindung hauptsächlich Schritte E1 bis E17 auf. Zu Anfang wurde die Mobilstation TM eingeschaltet und vom zellularen Netz RC in einer Zone erkannt, die von diesem funkelektrisch versorgt wird. Die Mobilstation TM im Standby-Zustand befindet sich so in einem Lokalisierungsbereich ZL des Netzes RC, und eine vorübergehende Identität TMSI wurde ihm von der Besucherdatei VLR zugeordnet, die diesem Lokalisierungsbereich in bekannter Weise zugeteilt ist.

[0030] Im Schritt E1 beschließt der Benutzer der Mobilstation TM, der in das Versorgungsgebiet des drahtlosen Netzes geringer Reichweite RFP mit den Zugriffspunkten AP eindringt, ein Bluetooth-Menü auf seiner Mobilstation TM zu wählen, und insbesondere ein Untermenü (inquiry mode) der Suche nach Zugriffspunkten AP. Die Zugriffspunkte AP in Form von Endgeräten können gesucht werden, d.h. erforschen je periodisch das Vorhandensein einer Mobilstation, um eine Abfrage (inquiry) zu erfassen, die von den Mobilstationen übertragen wird. Über diesen Umweg sammelt die Mobilstation TM die Adressen ADAP der Zugriffspunkte, die sich im Versorgungsgebiet der Mobilstation TM bezüglich des Netzes geringer Reichweite RFP befinden. Die Mobilstation TM sortiert unter den Antworten auf ihre Suche, die sie empfängt, die Adressen der Einheiten des Netzes geringer Reichweite RFP aus, die Vorrichtungsklassen entsprechen, die den Zugriffspunkten zugeordnet sind, um jede Adresse zu entfernen, die von einer beliebigen Vorrichtung kommt, die mit einem Sende-Empfangs-Modul ausgestattet ist, das mit dem RFP-Netz kompatibel ist, wie ein Mobiltelefon, ein Minicomputer PDA, ein Laptop, usw.

[0031] Im Schritt E2 werden die Adressen ADAP der verfügbaren und während der vorhergehenden Suche gefundenen Zugriffspunkte in der Mobilstation TM gespeichert und in eine Anfrage RQ eingefügt, die zur Verwaltungsplattform PFG über das Festnetz des zellularen Netzes RC zu übertragen ist. Die Anfrage RQ enthält die Adresse ADTM der Mobilstation TM, die vorher in dieser gespeichert wurde, damit die Plattform PFG sie den später ausgewählten Zugriffspunkten mitteilen kann. Die Anfrage RQ enthält als Zieladresse einen Identifikator IDPFG der Plattform PFG, der vorher in der Mobilstation TM gespeichert wurde. Die Anfrage RQ kann in Form einer Kurzmitteilung oder einer Signalisierungsnachricht USSD vorliegen, und die Plattform PFG ist dann mit der entsprechenden Mitteilungszentrale CM verbunden.

[0032] Wenn die Anfrage RQ automatisch von der Mobilstation TM gesendet und von der Plattform PFG empfangen wurde, untersucht die Plattform die Liste der Zugriffspunktadressen ADAP, die aus der Anfrage RQ entnommen wurde, um den optimalen Zugriffspunkt in Abhängigkeit von einem oder mehreren Kriterien auszuwählen, die im Schritt E3 vorbestimmt werden. Vor der Auswahl des optimalen Zugriffspunkts liegt eine Überprüfung des Profils des Benutzers der Mobilstation TM, der von seinem permanenten Identifikator IMSI identifiziert wird, um ihm zu erlauben, auf einen Zugriffspunkt des drahtlosen Netzes geringer Reichweite RFP zuzugreifen.

[0033] Gemäß einer ersten Variante bezieht sich ein vorbestimmtes Kriterium auf einen Vergleich von Leistungspegeln von den von der Mobilstation TM gefundenen Zugriffspunkten ausgesendeten Bezugssignalen, die von der Mobilstation TM empfangen werden. In dieser Variante umfasst die Mobilstation TM ebenfalls zusammen mit jeder Adresse

ADAP eines verfügbaren und in der übertragenen Anfrage RQ gefundenen Zugriffspunkts einen Leistungspegel NP, der in der Mobilstation empfangen wird. Die Mobilstation überträgt dann die Anfrage RQ mit Paaren ADAP, NP an die Verwaltungsplattform PFG, die die empfangenen Leistungspegel NP vergleicht, um den höchsten empfangenen Leistungspegel zu bestimmen und den dem höchsten empfangenen Leistungspegel zugeordneten Zugriffspunkt AP als optimalen Zugriffspunkt auszuwählen, um eine Verbindung mit der Mobilstation TM aufzubauen.

[0034] Gemäß einer der vorhergehenden in etwa ähnlichen Variante wird der optimale Zugriffspunkt mit dem höchsten Leistungspegel, der von der Mobilstation empfangen wird, gesucht und im Schritt E1 unter den verfügbaren und im Versorgungsgebiet der Mobilstation TM gefundenen Zugriffspunkte von der Mobilstation TM selbst anstelle der Plattform PFG ausgewählt. Die Anfrage RQ enthält nur die Adresse ADAP des optimalen Zugriffspunkts AP anstelle der Liste der Paare ADAP, NP.

[0035] Gemäß einer zweiten Variante bezieht sich ein vorbestimmtes Kriterium auf einen Vergleich von Verkehrslasten der verfügbaren und von der Mobilstation TM gefundenen Zugriffspunkte AP, damit die Verwaltungsplattform PFG den Zugriffspunkt mit der geringsten Verkehrslast als optimalen Zugriffspunkt auswählt. Die Verkehrslasten der Zugriffspunkte AP des Netzes geringer Reichweite RFP werden von dem Verteilernetz RD aufgefangen, das sie periodisch über das Internet RP oder eine spezialisierte Leitung an die Plattform PFG für eine Aktualisierung der Datenbasis bezüglich der Zugriffspunkte übermittelt.

[0036] Gemäß einer komplementären Variante, die mit der ersten oder zweiten vorhergehenden Variante zu kombinieren ist, fragt die Plattform PFG die Heimatdatei HLR des zellularen Netzes RC ab, um dort vor der Auswahl der Adresse des optimalen Zugriffspunkts den Identifikator IDZL des Lokalisierungsbereichs abzulesen, in dem sich die Mobilstation TM im zellularen Netz befindet. In Abhängigkeit vom Identifikator des Lokalisierungsbereichs IDZL entfernt die Plattform PFG die Adressen ADAP aus der in der Anfrage RQ enthaltenen Liste, die verfügbare und gefundene Zugriffspunkte AP definieren, die sich außerhalb des Lokalisierungsbereichs befinden, der die Mobilstation TM einschließt und im zellularen Netz definiert ist. Diese komplementäre Variante verhindert, dass eine Mobilstation den Platz des Zugriffspunkts einnimmt, indem sie sich mit einer Adresse eines Zugriffspunkts erklärt, der sehr weit von der Mobilstation entfernt ist, um mit dieser zu kommunizieren. Dann wird der optimale Zugriffspunkt von der Plattform PFG ausgewählt, entweder, indem sie einfach die Adresse des ersten Zugriffspunkts der aus der Anfrage RQ entnommen Liste nimmt, oder indem sie diese Variante mit der Variante der Leistungs- oder der Lastpegel der Zugriffspunkte kombiniert, um den Zugriffspunkt auszuwählen, der den höchsten Leistungspegel oder die geringste Verkehrlast unter denjenigen aufweist, die sich im Lokalisierungsbereich befinden.

[0037] Im Schritt E3 bestimmt der Pseudozufallsgenerator in der Verwaltungsplattform PFG ebenfalls einen Geheimcode CS, der eine große Länge von mindestens gleich 128 Bits hat.

[0038] Die Plattform PFG bereitet danach zwei Mitteilungen vor.

[0039] Im Schritt E4 wird eine Bestätigungsmitteilung MC, die die Adresse ADAP des optimalen Zugriffspunkts und den erzeugten Geheimcode CS enthält, von der Plattform PFG erstellt, um sie an die Mobilstation TM über das zellulare Netz RC zu übertragen. Die Mitteilung MC ist vom gleichen Typ wie die Anfrage RQ, d.h. eine Kurzmitteilung SM oder eine Mitteilung USSD, und geht über die entsprechende Mitteilungszentrale CM. Der aus der Mitteilung MC entnommene Geheimcode CS wird zusammen mit der Adresse des optimalen Zugriffspunkts ADAP in der Mobilstation TM gespeichert. Die Mobilstation TM besitzt im Schritt E4 den Geheimcode CS, als ob, gemäß dem Stand der Technik, der Benutzer den PIN-Code in die Tastatur der Mobilstation eingegeben hätte.

[0040] Parallel zum Schritt E4 erstellt die Plattform PFG im Schritt E5 eine Verbindungsanforderungsmitteilung MDC, die die Adresse ADTM der Mobilstation TM, die Adresse ADAP des optimalen Zugriffspunkts und den erzeugten Geheimcode CS für den optimalen Zugriffspunkt AP im drahtlosen Netz geringer Reichweite enthält. Die Verbindungsanforderungsmitteilung MDC liegt in Form eines IP-Pakets (Internet-Protokoll) vor, das über das Internet RP zum Verteilernetz RD des drahtlosen Netzes geringer Reichweite RFP geht. Der aus der Mitteilung MDC entnommene Geheimcode CS wird zusammen mit der Adresse ADTM im optimalen Zugriffspunkt AP gespeichert.

[0041] Als Antwort auf die Adresse ADAP des optimalen Zugriffspunkts AP, der aus der von der Mobilstation TM empfangenen Bestätigungsmitteilung MC entnommen wird, versucht diese, sich mit dem so identifizierten optimalen Zugriffspunkt AP zu verbinden, indem sie den optimalen Zugriffspunkt auffordert, sie zu authentifizieren. Im Schritt E6 sendet die Mobilstation TM einen ersten Rahmen T1, der die Adresse der Mobilstation ADTM, die Adresse ADAP des optimalen Zugriffspunkts und einen Indikator einer Verbindungsanforderung und der Bestimmung eines Sitzungsschlüssels DC enthält.

[0042] Der optimale Zugriffspunkt im Modus der periodischen Suche erkennt, dass der Rahmen T1 für ihn bestimmt ist. Die Mobilstation und der Zugriffspunkt bestimmen dann je einen gemeinsamen Sitzungsschlüssel KS, indem sie an den Sitzungsschlüsselalgorithmus AS die Adresse der Mobilstation ADTM, die Adresse ADAP des Zugriffspunkts, den Geheimcode CS und eine oder mehrere Zufallszahlen RAND anwenden, die zwischen ihnen über das Netz geringer Reichweite RFP ausgetauscht werden. Der in der Mobilstation verwendete Geheimcode CS ist derjenige, der aus der Bestätigungsmitteilung MC entnommen wird, während der im Zugriffspunkt AP verwendete Geheimcode CS derjenige ist, der aus der Verbindungsanforderungsmitteilung MDC entnommen wird. Die Mobilstation TM und der optimale Zugriffspunkt AP werden so paarweise miteinander verbunden. Der Sitzungsschlüssel KS wird in der Mobilstation und im Zugriffspunkt gespeichert und wird insbesondere für die Authentifizierung und eine Datenverschlüsselung nur bis zum Abschalten des Zugriffspunkts AP und der Mobilstation TM verwendet.

[0043] Die Authentifizierung der Mobilstation TM wird anschließend vom optimalen Zugriffspunkt ausgelöst, indem er im Schritt E7 als Antwort auf den ersten Rahmen T1 einen Rahmen T2 sendet, der die Adresse des optimalen Zugriffspunkts ADAP, die Adresse ADTM der Mobilstation TM, eine vom Pseudozufallsgenerator im Zugriffspunkt erzeugte Zufallszahl RAP und einen Antwortanforderungsindikator DRP zur Mobilstation TM enthält.

[0044] Das Verfahren geht dann zu Schritten E8, E9 und E10 bezüglich einer eigentlichen Authentifizierung der Mobilstation TM durch den optimalen Zugriffspunkt AP über. Bei Empfang des Rahmens T2 mit dem Antwortanforderungsindikator wendet die Mobilstation TM im Schritt E8 die aus dem Rahmen T2 entnommene Zufallszahl RAP, den im Schritt E6 bestimmten Sitzungsschlüssel KS und seine Adresse ADTM an den Authentifizierungsalgorithmus AA an, der eine Antwort RP1 erzeugt. Ebenfalls im Schritt E8 führt der optimale Zugriffspunkt AP eine analoge Anwendung durch: RP1 = AA (RAP, KS, ADTM), bei der aber der Sitzungsschlüssel derjenige ist, den er im Schritt E6 bestimmt und der Adresse ADTM zugeordnet hat. Dann sendet die Mobilstation im Schritt E9 einen Rahmen T3, der außer den Adressen ADTM und ADAP die Antwort RP1 = AA (RAP, KS, ADTM) enthält, die in der Mobilstation bestimmt wurde. Der Rahmen T3 wird vom optimalen Zugriffspunkt AP erkannt, der im Schritt E10 die im optimalen Zugriffspunkt bestimmte Antwort RP1 mit der Antwort RP1 vergleicht, die aus dem empfangenen Rahmen T3 entnommen wird. Wenn die verglichenen Antworten RP1 gleich sind, erlaubt der optimale Zugriffspunkt AP im Schritt E16 die Eröffnung einer Sitzung über diesen von der Mobilstation TM zum Verteilungsnetz RD und dem Internet RP.

[0045] Der Sitzungsschlüssel KS für diese eröffnete Sitzung wird verwendet, um den Sitzungsschlüssel einer folgenden Sitzung zwischen der Mobilstation TM und dem Zugriffspunkt AP zu bestimmen, wenn der Sitzungsschlüssel KS nicht zwischenzeitlich bei Ablauf einer Zeitdauer ausgehend von der Speicherung des Schlüssels KS gelöscht wurde, die vom dem den Zugriffspunkt verwaltenden Betreiber vorherbestimmt wurde.

[0046] Gemäß einer vollständigeren Variante bezüglich einer gegenseitigen Authentifizierung, wenn der optimale Zugriffspunkt AP die Mobilstation TM im Schritt E10 authentifiziert hat, sendet der optimale Zugriffspunkt AP im Schritt E11 einen Rahmen T4, der die Adressen ADAP und ADTM und einen Indikator IA enthält, um die Mobilstation TM aufzufordern, ihn zu authentifizieren.

[0047] Als Antwort auf den vorhergehenden Rahmen T4 löst die Mobilstation TM die Authentifizierung des optimalen Zugriffspunkts aus, indem sie einen Rahmen T5 aussendet, der für den optimalen Zugriffspunkt der Adresse ADAP bestimmt ist. Der Rahmen T5 enthält eine Zufallszahl RTM, die vom Pseudozufallsgenerator in der Mobilstation erzeugt wird, und einen Antwortanfrageindikator DRP im Schritt E12. Nach dem Rahmen T5, im Schritt E13, wendet der Zugriffspunkt AP die aus dem Rahmen T5 entnommene Zufallszahl RTM, den im Schritt E6 bestimmten Sitzungsschlüssel KS und seine Adresse ADAP an den Authentifizierungsalgorithmus AA an, der eine zweite Antwort RP2 erzeugt. Ebenfalls im Schritt E13 führt die Mobilstation TM eine Anwendung RP2 = AA (RTM, KS, ADAP) aus, bei der aber der Sitzungsschlüssel derjenige ist, den sie im Schritt E6 bestimmt und der Adresse ADAP zugeordnet hat. Dann sendet der optimale Zugriffspunkt AP einen Rahmen T6, der außer den Adressen ADAP und ADTM die Antwort RP2 = AA (RTM, KS, ADAP) enthält, die im optimalen Zugriffspunkt bestimmt wurde. Der Rahmen T6 wird von der Mobilstation TM erkannt, die im Schritt E15 die in der Mobilstation bestimmte Antwort RP2 mit der Antwort RP2 vergleicht, die aus dem empfangenen Rahmen T6 entnommen wurde. Wenn die verglichenen Antworten RP2 gleich sind, bestätigt die Mobilstation TM im Schritt E16 durch das Senden eines weiteren Rahmens die Eröffnung der angeforderten Sitzung an den optimalen Zugriffspunkt AP.

[0048] In einer Variante wird der Sitzungsschlüssel KS nicht getrennt von der Mobilstation TM und dem optimalen Zugriffspunkt AP im Schritt E6, sondern vorher durch die Verwaltungsplattform PFG im Schritt E3 bestimmt. Die Plattform erzeugt zufällig einen Sitzungsschlüssel KS der gleichen Größe wie derjenige gemäß der vorher beschriebenen Ausführung.

[0049] Um eine Kohärenz zu gewährleisten, kann

die Plattform aber den Sitzungsschlüsselalgorithmus AS enthalten. Am Ende des Schritts E3 hat die Plattform den optimalen Zugriffspunkt ausgewählt und hat die Adresse ADAP des optimalen Zugriffspunkts der Adresse ADTM der Mobilstation zugeordnet, die aus der Anfrage RQ entnommen wurde, was es ihr ermöglicht, den Sitzungsschlüssel zu bestimmen, indem sie die Adressen ADAP und ADTM, den Geheimcode CS und eine oder mehrere Zufallszahlen RAND an den Algorithmus AS anlegt, d.h.:

KS = AS (ADAP, ADTM, CS, RAND).

[0050] In den Schritten E4 und E5 führt die Verwaltungsplattform PFG den bestimmten Sitzungsschlüssel KS anstelle des Geheimcodes CS in die Bestätigungsmitteilung MC, die an die Mobilstation übertragen wird, und in die Verbindungsanforderungsmitteilung MDC ein, die an den optimalen Zugriffspunkt übertragen wird, damit der optimale Zugriffspunkt und die Mobilstation den Sitzungsschlüssel KS zur Authentifizierung E6 bis E10 oder E6 bis E15 und nach der im Schritt E16 eröffneten Sitzung verwenden, wobei der Schritt E6 keine Bestimmung des Sitzungsschlüssels KS mehr aufweist.

[0051] Wie im Schritt E17 angegeben, wenn die Authentifizierung der Mobilstation durch den optimalen Zugriffspunkt fehlgeschlagen ist, d.h. wenn die im Schritt E10 verglichenen Antworten RP1 unterschiedlich sind, oder wenn die gegenseitige Authentifizierung fehlgeschlagen ist, d.h. wenn die im Schritt E15 verglichenen Antworten RP2 unterschiedlich sind, wird ein Versuch einer Anforderung der Eröffnung einer Sitzung wiederholt, indem die Schritte E6 bis E10 gemäß der Ausführung mit Authentifizierung der Mobilstation durch den optimalen Zugriffspunkt oder die Schritte E6 bis E15 gemäß der Variante mit gegenseitiger Authentifizierung durchgeführt werden.

[0052] In der Praxis können die Schritte der Verbindungsanforderung, der Bestimmung von Antworten und des Vergleichs von Antworten E6 bis E10 oder E6 bis E15 maximal N Mal wiederholt werden, so lange die verglichenen Antworten RP1 oder RP2 unterschiedlich sind, wobei N eine vorbestimmte Anzahl von Wiederholungen ist, zum Beispiel 3.

[0053] Wenn nach N Wiederholungen einer Verbindungsanforderung im Schritt E17 die Authentifizierung fehlgeschlagen ist, d.h. die verglichenen Antworten noch unterschiedlich sind, kann das Verfahren automatisch in den Schritt E2 zurückkommen, um die folgenden Schritte E3 bis E17 bezüglich der Adresse ADAP eines anderen Zugriffspunkts auszuführen, der gemäß den vorbestimmten Kriterien zum Beispiel in der Liste ausgewählt wird, die in der Anfrage RQ enthalten ist, wie in einem Zwischenschritt E18 angegeben ist. Die Auswahl dieses anderen Zugriffspunkts in der Liste schließt natürlich den letzten optimalen Zugriffspunkt aus, der vorher ausgewählt wurde und für den N Verbindungsversuche fehlgeschlagen sind. Der andere ausgewählte optimale Zugriffspunkt befindet sich im Versorgungsgebiet der Mobilstation TM bezüglich des Netzes geringer Reichweite RFP und kann der Zugriffspunkt sein, der den höchsten empfangenen Leistungspegel oder die kleinste Verkehrslast in der verbleibenden Liste aufweist, oder derjenige, der auf den letzten optimalen Zugriffspunkt folgt, der in der Liste ausgewählt wurde.

[0054] Obwohl die Erfindung für ein zellulares Netz vom Typ GSM und für ein drahtloses Netz geringer Reichweite vom Typ Bluetooth beschrieben wurde, kann die Erfindung ebenfalls im Kontext eines Funkverkehrsnetzes für Mobiltelefone vom Typ UMTS oder allgemeiner vom Typ dritte Generation und auf andere drahtlose Netze geringer Reichweite zum Beispiel von dem Typ gemäß der Norm IEEE 802.11b und gemäß den anderen auf diese folgenden Normen angewendet werden, d.h. für Netze, die auch Wi-Fi-Netze (Wireless Fidelity) genannt werden.

Patentansprüche

1. Authentifizierungsverfahren zwischen einem drahtlosen Netz geringer Reichweite (RFP) mit Zugriffspunkten und einer Mobilstation (TM) in einem zellularen Funkverkehrsnetz (RC), **dadurch gekennzeichnet**, dass es die folgenden Schritte aufweist:
– Übertragung (E2) einer Anfrage (RQ), die eine Adresse (ADTM) der Mobilstation und eine Adresse (ADAP) eines Zugriffspunkts (AP) enthält, der sich im Versorgungsgebiet der Mobilstation (TM) bezüglich des Netzes geringer Reichweite befindet, von der Mobilstation über das zellulare Netz (RC) zu einer Verwaltungseinrichtung (PFG),
– Bestimmung (E3) eines Geheimcodes (CS) durch die Verwaltungseinrichtung,
– ausgehend von der Verwaltungseinrichtung (PFG), Übertragung (E4, E5) einer Bestätigungsmitteilung (MC), die den Geheimcode und die aus der Anfrage entnommene Adresse des Zugriffspunkts enthält, an die Mobilstation über das zellulare Netz, und einer Verbindungsanforderungsmitteilung (MDC), die den Geheimcode und die aus der Anfrage entnommene Adresse der Mobilstation enthält, an den Zugriffspunkt (AP),
– Anforderung (E6) einer Verbindung von der Mobilstation zu dem von der aus der Bestätigungsmitteilung (MC) entnommenen Adresse (ADAP) bezeichneten Zugriffspunkt, damit die Mobilstation (TM) und der Zugriffspunkt (AP) in Abhängigkeit von der Adresse (ADAP) des Zugriffspunkts, der Adresse (ADTM) der Mobilstation und vom aus der Bestätigungsmitteilung (MC) und aus der Verbindungsanforderungsmitteilung (MDC) entnommenen Geheimcode (CS) einen Sitzungsschlüssel (KS) bestimmen, und
– Authentifizierung (E7-E10) der Mobilstation (TM) durch den Zugriffspunkt (AP) in Abhängigkeit vom

Sitzungsschlüssel (KS).

2. Verfahren nach Anspruch 1, gemäß dem die Authentifizierung der Mobilstation durch den Zugriffspunkt ausgehend vom Zugriffspunkt eine Anforderung (E7) der Bestimmung (E8) einer Antwort (RP1) in Abhängigkeit vom Sitzungsschlüssel (KS) an die Mobilstation, die die Antwort über das Netz geringer Reichweite an den Zugriffspunkt überträgt (E9), und im Zugriffspunkt (AP) eine Bestimmung (E8) einer Antwort (RP1) in Abhängigkeit vom Sitzungsschlüssel (KS) und einen Vergleich (E10) der Antworten enthält, um die Eröffnung einer Sitzung zwischen dem Zugriffspunkt und der Mobilstation zu erlauben (E16), wenn mindestens die verglichenen Antworten gleich sind.

3. Verfahren nach Anspruch 1 oder 2, das eine Authentifizierung (E11-E15) des Zugriffspunkts (AP) durch die Mobilstation (TM) in Abhängigkeit vom Sitzungsschlüssel (KS) aufweist, wenn der Zugriffspunkt die Mobilstation authentifiziert hat.

4. Verfahren nach Anspruch 3, gemäß dem die Authentifizierung des Zugriffspunkts durch die Mobilstation eine Aufforderung (E11) durch den Zugriffspunkt enthält, die an die Mobilstation (TM) übertragen wird, damit die Mobilstation den Zugriffspunkt authentifiziert, indem sie vom Zugriffspunkt fordert (E12), eine zweite Antwort (RP2) in Abhängigkeit vom Sitzungsschlüssel (KS) zu bestimmen (E13) und die zweite Antwort über das Netz geringer Reichweite (RFP) an die Mobilstation zu übertragen (E14), indem sie eine zweite Antwort (RP2) in Abhängigkeit vom Sitzungsschlüssel (KS) bestimmt (E13), und indem sie die zweiten Antworten (RP2) vergleicht (E15), damit die Eröffnung der Sitzung erst nach einer Identität der in der Mobilstation verglichenen zweiten Antworten erlaubt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, das maximal eine vorbestimmte Anzahl von Iterationen (E17) der Schritte der Verbindungsanforderung und der Authentifizierung (E6-E10; E6-E15) aufweist, solange die Authentifizierung fehlgeschlagen ist.

6. Verfahren nach Anspruch 5, das eine Iteration (E18) der in Anspruch 1 aufgezählten Schritte (E2-E17) bezüglich eines anderen Zugriffspunkts (AP) im Versorgungsgebiet der Mobilstation (TM) enthält, wenn die Authentifizierung eine vorbestimmte Anzahl von Malen fehlgeschlagen ist (E17).

7. Verfahren nach einem der Ansprüche 1 bis 6, das in der Mobilstation (TM) eine Suche (E1) nach einem optimalen Zugriffspunkt (AP) mit dem größten Leistungspegel enthält, der von der Mobilstation unter Zugriffspunkten im Versorgungsgebiet der Mobilstation empfangen wird, damit die Mobilstation (TM) die Adresse (ADAP) des optimalen Zugriffspunkts in die Anfrage (RQ) einfügt.

8. Verfahren nach einem der Ansprüche 1 bis 6, das in der Mobilstation (TM) eine Suche (E1) nach Zugriffspunkten im Versorgungsgebiet der Mobilstation, um Adressen (ADAP) der gefundenen Zugriffspunkte in die Anfrage (RQ) einzufügen, und in der Verwaltungseinrichtung (PFG) eine Auswahl (E3) der Adresse (ADAP) eines optimalen Zugriffspunkts (AP) unter den Zugriffspunktadressen aufweist, die aus der Anfrage (RQ) gemäß einem vorbestimmten Kriterium entnommen wurden, um die Adresse des optimalen Zugriffspunkts in die Bestätigungsmitteilung (MC), die an die Mobilstation übertragen wird, und in die Verbindungsanforderungsmitteilung (MDC) einzufügen, die an den optimalen Zugriffspunkt (AP) übertragen wird.

9. Verfahren nach Anspruch 8, gemäß dem das vorbestimmte Kriterium sich auf einen Leistungspegelvergleich (NP) der gefundenen Zugriffspunkte (AP) bezieht, die von der Mobilstation (TM) empfangen und zusammen mit den Adressen (ADAP) der in der Anfrage (RQ) gefundenen Zugriffspunkte übertragen werden, damit die Verwaltungseinrichtung (PFG) den empfangenen Zugriffspunkt mit dem größten Leistungspegel als optimalen Zugriffspunkt bestimmt.

10. Verfahren nach Anspruch 8 oder 9, gemäß dem das vorbestimmte Kriterium sich auf einen Vergleich von Verkehrslasten der von der Mobilstation (TM) gefundenen (E1) Zugriffspunkte (AP) bezieht, damit die Verwaltungseinrichtung (PFG) den Zugriffspunkt mit der geringsten Last als optimalen Zugriffspunkt wählt.

11. Verfahren nach einem der Ansprüche 8 bis 10, gemäß dem das vorbestimmte Kriterium sich außerdem auf eine Unterdrückung der Adressen (ADAP) der gefundenen Zugriffspunkte (AP), die sich außerhalb eines die Mobilstation (TM) einschließenden und im zellularen Netz (RC) definierten Lokalisierungsbereichs befinden, vor der Auswahl der Adresse des optimalen Zugriffspunkts bezieht.

12. Verfahren nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass der von der Verwaltungseinrichtung (PFG) bestimmte Geheimcode (CS) pseudozufällig erzeugt wird und eine Länge von mehr als 16 Bytes hat.

13. Verfahren nach einem der Ansprüche 1 bis 12, das in der Verwaltungseinrichtung (PFG) eine Bestimmung (E3) des Sitzungsschlüssels (KS) anstelle der Bestimmungen (E6) des Sitzungsschlüssels in der Mobilstation (TM) und im Zugriffspunkt (AP), und eine Einführung (E4, E5) des bestimmten Sitzungsschlüssels (KS) anstelle des Geheimcodes in die Bestätigungsmitteilung (MC) und die Verbindungsanfor-

derungsmitteilung (MDC) aufweist.

14. Authentifizierungssystem zwischen einem drahtlosen Netz geringer Reichweite (RDFP) mit Zugriffspunkten und einer Mobilstation (TM) in einem zellularen Funkverkehrsnetz (RC), dadurch gekennzeichnet, dass es aufweist:
eine Verwaltungseinrichtung (PFG), um einen Geheimschlüssel (CS) als Antwort auf eine Anfrage (RQ) zu bestimmen, die die Adresse (ADTM) der Mobilstation und die Adresse (ADAP) eines Zugriffspunkts (AP) enthält, der sich im Versorgungsgebiet der Mobilstation (TM) bezüglich des Netzes geringer Reichweite befindet, und die von der Mobilstation über das zellulare Netz (RC) übertragen wird, um eine Bestätigungsmitteilung (MC), die den Geheimschlüssel und die aus der Anfrage (RQ) entnommene Adresse des Zugriffspunkts enthält, über das zellulare Netz (RC) an die Mobilstation (TM), und eine Verbindungsanforderungsmitteilung (MDC), die den Geheimcode und die aus der Anfrage entnommene Adresse (ADTM) der Mobilstation enthält, an den Zugriffspunkt (AP) zu übertragen,
die Mobilstation, um eine Verbindung mit dem von der aus der Bestätigungsmitteilung (MC) entnommenen Adresse (ADAP) bezeichneten Zugriffspunkt (AP) anzufordern, und um einen Sitzungsschlüssel (KS) in Abhängigkeit von der Adresse (ADAP) des Zugriffspunkts, der Adresse (ADTM) der Mobilstation und dem aus der Bestätigungsmitteilung (MC) entnommenen Geheimcode (CS) zu bestimmen, und
den Zugriffspunkt (AP), um den Sitzungsschlüssel (KS) in Abhängigkeit von der Adresse (ADAP) des Zugriffspunkts, der Adresse (ADTM) der Mobilstation und dem aus der Verbindungsanforderungsmitteilung (MDC) entnommenen Geheimcode (CS) zu bestimmen, und um die Mobilstation in Abhängigkeit vom Sitzungsschlüssel (KS) zu authentifizieren.

15. System nach Anspruch 14, dadurch gekennzeichnet, dass die Verwaltungseinrichtung selbst den Sitzungsschlüssel bestimmt und ihn anstelle des Geheimcodes in die Bestätigungsmitteilung (MC) und die Verbindungsanforderungsmitteilung (MDC) einfügt.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

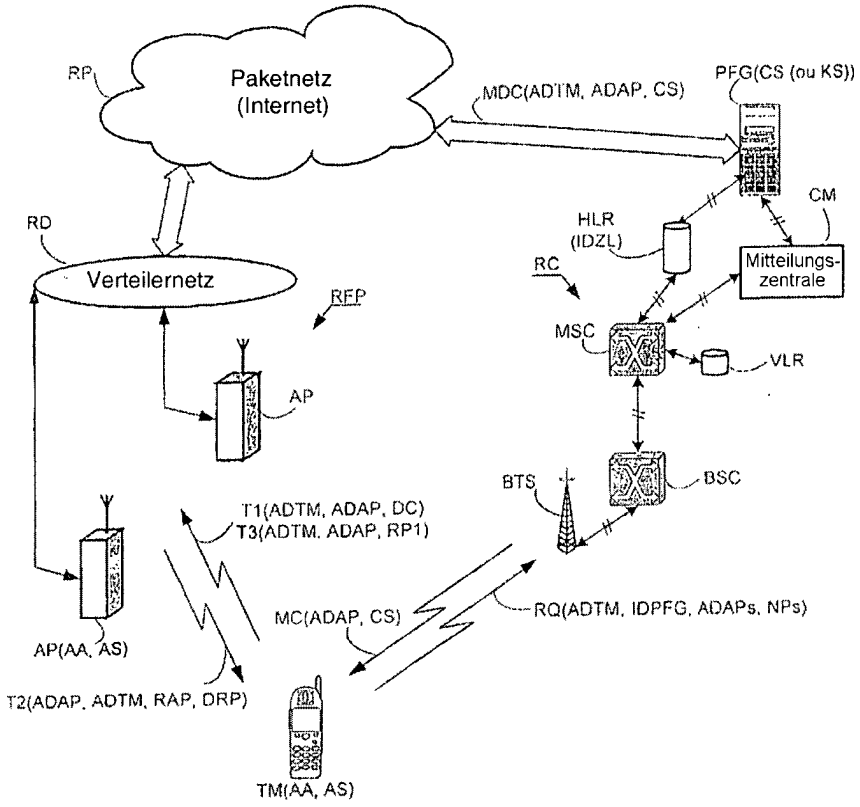
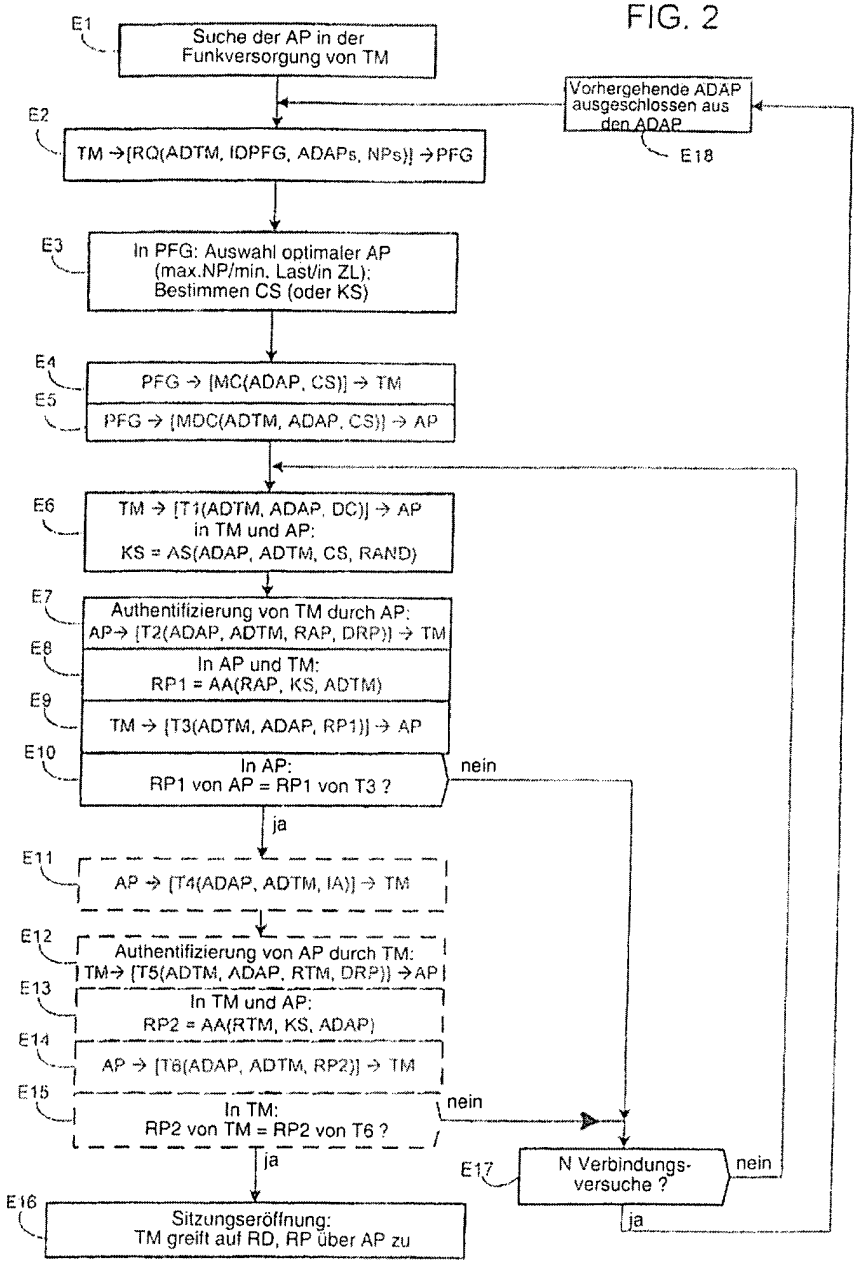


FIG. 2


E1
Suche der AP in der Funkversorgung von TM
Vorhergehende ADAP ausgeschlossen aus den ADAP
E18
E2
TM →[RQ(ADTM, IDPFG, ADAPs, NPs)] →PFG
E3
In PFG: Auswahl optimaler AP (max.NP/min. Last/in ZL): Bestimmen CS (oder KS)
E4
PFG → [MC(ADAP, CS)] → TM
E5
PFG → [MDC(ADTM, ADAP, CS)] → AP
E6
TM → [T1(ADTM, ADAP, DC)] → AP
in TM und AP:
KS = AS(ADAP, ADTM, CS, RAND)
E7
Authentifizierung von TM durch AP:
AP→ [T2(ADAP, ADTM, RAP, DRP)] → TM
E8
In AP und TM:
RP1 = AA(RAP, KS, ADTM)
E9
TM → [T3(ADTM, ADAP, RP1)] → AP
E10
In AP:
RP1 von AP = RP1 von T3 ?
nein
ja
E11
AP → [T4(ADAP, ADTM, IA)] → TM
E12
Authentifizierung von AP durch TM:
TM→ [T5(ADTM, ADAP, RTM, DRP)] →AP
E13
In TM und AP:
RP2 = AA(RTM, KS, ADAP)
E14
AP → [T6(ADAP, ADTM, RP2)] → TM
E15
In TM:
RP2 von TM = RP2 von T6 ?
nein
ja
E16
Sitzungseröffnung:
TM greift auf RD, RP über AP zu
E17
N Verbindungs-versuche ?
nein
ja