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

(10) **DE 603 17 849 T2** 2008.12.11

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 367 776 B1**
(21) Deutsches Aktenzeichen: **603 17 849.9**
(96) Europäisches Aktenzeichen: **03 291 176.0**
(96) Europäischer Anmeldetag: **20.05.2003**
(97) Erstveröffentlichung durch das EPA: **03.12.2003**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **05.12.2007**
(47) Veröffentlichungstag im Patentblatt: **11.12.2008**

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

(30) Unionspriorität:
0206641 **30.05.2002** **FR**

(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

(73) Patentinhaber:
Alcatel Lucent, Paris, FR

(74) Vertreter:
Patentanwälte U. Knecht und Kollegen, 70435 Stuttgart

(72) Erfinder:
Loeffler, Siegfried, 75014 Paris, FR; Laine, Philippe, 92130 Issy-les-Moulineaux, FR; Sehier, Philippe, 78100 Saint Germain en Laye, FR

(54) Bezeichnung: **Zugriffskontrollverfahren und -gerät für ein drahtloses LAN**

Beschreibung

[0001] Die vorliegende Erfindung bezieht sich auf den Bereich der Kommunikation zwischen Endgeräten innerhalb von Netzwerken, und insbesondere auf die Kontrolle und den Zugriff auf ein drahtloses lokales Netzwerk.

[0002] Die Mobilfunkbetreiber stellen ihren Kunden, die über mobile Kommunikationsendgeräte verfügen, zahlreiche Dienste zur Verfügung, wie beispielsweise den Zugriff auf ein öffentliches Netzwerk wie das Internet oder auf private Netzwerke wie z. B. das Intranet eines Unternehmens. Aufgrund der hohen Dichte an mobilen Kommunikationsendgeräten, die an bestimmten Orten, so genannten „Hot Spots", gleichzeitig genutzt werden, beispielsweise in Bahnhöfen oder auf Flughäfen, sind jedoch einerseits die Zugriffszeiten auf diese Dienste oft sehr lang, und andererseits kommt es häufig zu Unterbrechungen.

[0003] Eine bekannte Lösung, diesen Nachteil zu beseitigen, besteht darin, bestimmten mobilen Endgeräten zu ermöglichen, eine Verbindung mit bereits vorhandenen drahtlosen lokalen Kommunikationsnetzwerken (besser bekannt unter der englischen Abkürzung WLAN für „Wireless Local Area Network") herzustellen, insbesondere an bestimmten Hot Spots, und über einen Provider auf das Internet sowie manchmal über das Internet auf ein Intranet zuzugreifen. Um eine Verbindung mit einem WLAN herstellen zu können, muss der Nutzer allerdings zunächst wissen, dass er sich in einem WLAN-Abdeckungsbereich befindet und berechtigt ist, sich mit seinem mobilen Endgerät in dieses WLAN einzuloggen.

[0004] Andererseits muss das WLAN diesen Nutzer authentifizieren können. Sein mobiles Endgerät muss nicht nur mit der herkömmlichen Hardware für den Zugriff auf diese Art von Netzwerken ausgerüstet sein (wie z. B. mit einer auswechselbaren oder integrierten WLAN-Karte), sondern auch mit speziellen Zusatzgeräten, insbesondere mit einem Lesegerät für eine zweite SIM-Karte, die dazu dient, eine ausreichende Nutzungssicherheit für den Endnutzer zu gewährleisten. Diese speziellen Zusatzgeräte erhöhen die Größe und/oder das Gewicht des mobilen Endgeräts. Außerdem müssen sie vom Nutzer bezahlt werden, da sie nicht serienmäßig installiert sind.

[0005] Im Dokument GB 2.313.257 wird ein Verfahren beschrieben, das einem Nutzer die Möglichkeit bietet zu erfahren, wenn er sich im Abdeckungsbereich eines WLAN befindet, dabei muss dieser Nutzer jedoch die Initiative ergreifen, um eine Verbindung mit einem Server herzustellen, der mit diesem Hauptnetz verbunden ist, um zu erfahren, dass er sich im Abdeckungsbereich eines lokalen Netzwerks befindet, auf das er zugreifen könnte. Entweder erfasst das Endgerät seine Position (beispielsweise mit einem GPS-Empfänger) und gibt dem Server seine Ortsbestimmung an; dabei berücksichtigt der Server diese Ortsbestimmung, um gegebenenfalls die Daten zu übermitteln, die ein lokales Netzwerk oder die lokalen Netzwerke identifizieren, deren Abdeckungsbereiche die Position des Endgeräts abdecken. Oder der Server liefert Daten, die die Abdeckungsbereiche von lokalen Netzen definieren, die an zahlreichen Orten vorhanden sind, und das Endgerät muss seine Position selbst mit den Abdeckungsbereichen dieser lokalen Netzwerke vergleichen, um selbst zu ermitteln, ob es sich in einem Abdeckungsbereich befindet. Dieses bekannte Verfahren weist den Nachteil auf, dass der Nutzer die Initiative ergreifen muss, um eine Verbindung mit einem Server herzustellen.

[0006] Die Erfindung hat daher zum Ziel, die vorgenannten Nachteile ganz oder teilweise zu beseitigen. Zu diesem Zweck schlägt sie ein Verfahren zur Zugriffskontrolle für mindestens ein drahtloses lokales Netzwerk (WLAN-i) vor, das einen lokalen Abdeckungsbereich aufweist, der zumindest teilweise im Hauptabdeckungsbereich mindestens eines Haupt-Kommunikationsnetzwerks beinhaltet ist, das aus folgenden Schritten besteht:

– Ermittlung der Position zumindest einiger mobiler Kommunikationsendgeräte, die Kunden des genannten Hauptnetzwerks gehören, die sich im Hauptbereich aufhalten;
– Erfassung der mobilen Endgeräte, deren Position sich innerhalb des lokalen Abdeckungsbereichs des drahtlosen lokalen Kommunikationsnetzwerks befindet,
– und Adressierung einer Meldung an mindestens ein erfasstes mobiles Endgerät über das genannte Hauptnetzwerk, in der der Nutzer darauf hingewiesen wird, dass er sich im lokalen Bereich eines lokalen Netzwerks befindet, in das er sich einloggen kann;
dadurch gekennzeichnet:
– dass die Erfassung eines mobilen Endgeräts, dessen Position sich innerhalb des lokalen Abdeckungsbereichs eines drahtlosen lokalen Kommunikationsnetzwerks befindet, darin besteht, die Position jedes mobilen Endgeräts in den Verwaltungseinrichtungen des Hauptnetzwerks mit der Position mindestens eines lokalen Bereichs zu vergleichen,
– und dadurch, dass die Adressierung einer Meldung an ein mobiles Endgerät, das erfasst wurde, darin besteht, in den Verwaltungseinrichtungen des Hauptnetzwerks aus den primären Kennungen, die die mobilen Endgeräte kennzeichnen, diejenigen auszuwählen, die sich ungefähr in diesem lokalen Bereich befinden.

[0007] Unter „ungefähr" in dem lokalen Bereich befinden versteht man hier die Tatsache, sich entweder innerhalb des lokalen Bereichs oder in der Nähe

(oder in der unmittelbaren Umgebung) dieses lokalen Bereichs aufzuhalten. Im Übrigen versteht man hier unter einem mobilen Kommunikationsendgerät jedes mobile Endgerät (oder Gerät), das Meldungen vom Hauptnetzwerk des Mobilfunkbetreibers empfangen kann, zu dem sein mobiles Endgerät gehört. Dieses Endgerät verfügt vorzugsweise über Zugriffseinrichtungen für ein drahtloses lokales Netzwerk vom Typ WLAN. Dies ist jedoch nicht zwingend erforderlich. Bei dem mobilen Endgerät, das die Meldung empfängt, kann es sich natürlich auch beispielsweise um ein „herkömmliches" Mobiltelefon handeln, das einer Person gehört, die über ein anderes mobiles Endgerät verfügt, das mit Zugriffseinrichtungen für ein drahtloses lokales Netzwerk ausgerüstet ist. Bei diesem anderen mobilen Endgerät kann es sich beispielsweise um einen Laptop oder ein PDA handeln, die mit einer auswechselbaren oder integrierten Karte gemäß der Norm vom Typ 802.11 ausgerüstet sind.

[0008] Somit muss der Nutzer/Kunde sein mobiles Endgerät nicht speziell anpassen. Jedes Mal, wenn er sich innerhalb oder in der Nähe eines drahtlosen lokalen Netzwerks befindet, empfängt er vom Telefonbetreiber des Hauptnetzwerks, dessen Kunde er ist, automatisch auf einem seiner mobilen Endgeräte eine Meldung, z. B. eine SMS (für „Short Messaging System"). Anschließend kann er über das drahtlose lokale Netzwerk eine Zugriffsanforderung übermitteln.

[0009] Nach der Phase zur Auswahl der primären Kennung(en) wird vorzugsweise auf eine erste Zuordnungstabelle zwischen den primären Kennungen der mobilen Endgeräte und den Zugriffsberechtigungen (und/oder Zugriffsinteressen) für die lokalen Netzwerke zugegriffen, um unter den ausgewählten primären Kennungen diejenigen zu erfassen, die über eine Zugriffsberechtigung für das lokale Netzwerk in dem lokalen Bereich verfügen, in dem sich das entsprechende mobile Endgerät befindet. In diesem Fall werden nur an die mobilen Endgeräte Meldungen versandt, deren primäre Kennungen ausgewählt wurden.

[0010] Diese Zugriffsanforderung umfasst vorzugsweise ebenfalls ein Verfahren zur Authentifizierung der Kennung(en). Zu diesem Zweck kann jede Meldung eine sekundäre Kennung beinhalten, z. B. ein Passwort, vorzugsweise zum einmaligen Gebrauch, die an das drahtlose lokale Netzwerk beim Verbindungsversuch des mobilen Endgeräts mit diesem lokalen Netzwerk übermittelt werden muss. Zu diesem Zweck ist eine zweite Zuordnungstabelle zwischen sekundären Kennungen und tertiären Kennungen, wie beispielsweise Nutzernamen, vorgesehen, auf die beim Empfang einer sekundären Kennung, die einer tertiären Kennung zugeordnet ist, zugegriffen wird, um die Authentifizierung durchzuführen. Im Fall der Authentifizierung gibt man dem mobilen Endgerät den Zugriff auf das lokale Netzwerk frei. Diese Freigabe kann entweder für eine Sitzung mit unbeschränkter Dauer, für eine zeitlich begrenzte Sitzung oder für ein bestimmtes Datenübertragungsvolumen gewährt werden.

[0011] Im Fall einer gesicherten Zugriffsanforderung für ein drahtloses lokales Netzwerk wird im Übrigen vorzugsweise ein gesicherter Verbindungstunnel, wie z. B. ein gesicherter „IPsec-Tunnel", zwischen dem privaten Netzwerk und dem lokalen Netzwerk erstellt.

[0012] Beim Zugriff eines mobilen Endgeräts auf einen kostenpflichtigen Dienst über ein lokales Netzwerk kann man außerdem die Zahlungsdaten für diesen Dienst erfassen, um diese über das Hauptnetzwerk, dem der Kunde angehört, zu fakturieren.

[0013] Die Erfindung bezieht sich außerdem auf ein Gerät zur Zugriffskontrolle auf mindestens ein drahtloses lokales Kommunikationsnetzwerk, das einen lokalen Abdeckungsbereich aufweist, der zumindest teilweise im Hauptabdeckungsbereich mindestens eines Haupt-Kommunikationsnetzwerks enthalten ist, das mit Positionseinrichtungen für mobile Kommunikationsendgeräte ausgerüstet ist, wie beispielsweise einem LBS (für „Location Based Service").

[0014] Dieses Gerät ist durch die Tatsache gekennzeichnet, dass es Verwaltungseinrichtungen umfasst, die mit den Positionseinrichtungen verbunden und in der Lage sind:

- Die Position zumindest bestimmter mobiler Endgeräte mit der mindestens eines lokalen Bereichs zu vergleichen, um die primären Kennungen der mobilen Endgeräte auszuwählen, die sich ungefähr innerhalb dieses lokalen Bereichs befinden; und
- Dem E-Mail-Server des Hauptnetzwerks, mit dem das ausgewählte mobile Endgerät verbunden ist, Anweisungen zu übermitteln, die zumindest seine primäre Kennung beinhalten, so dass er diesem mobilen Endgerät über sein Hauptnetzwerk eine Meldung senden kann, in der dem Nutzer mitgeteilt wird, dass er sich innerhalb des lokalen Bereichs eines lokalen Netzwerks befindet, in das er sich einloggen kann.

[0015] Vorzugsweise umfasst das Gerät außerdem einen ersten Speicher, in dem eine erste Zuordnungstabelle zwischen den primären Kennungen der mobilen Endgeräte und den Zugriffsberechtigungen (und/oder den Zugriffsinteressen) für die lokalen Netzwerke gespeichert ist. In diesem Fall ist das Verwaltungsmodul mit dem ersten Speicher verbunden und in der Lage, auf die erste Zuordnungstabelle zuzugreifen, um unter den ausgewählten primären Kennungen diejenigen zu erfassen, die über eine Zu-

griffsberechtigung und/oder ein Interesse verfügen, auf das lokale Netzwerk in dem lokalen Bereich zuzugreifen, in dem sich das entsprechende mobile Endgerät befindet.

[0016] Die Verwaltungseinrichtungen können ebenfalls vorzugsweise Anweisungen an den betreffenden E-Mail-Server adressieren, die außerdem eine zugeordnete sekundäre Kennung umfassen, wie beispielsweise ein Passwort, das für den Nutzer des erfassten oder ausgewählten mobilen Endgeräts spezifisch ist, wobei diese sekundäre Kennung im Fall eines Einwahlversuchs in dieses lokale Netzwerk von dem mobilen Endgerät entsprechend einem der Zugriffspunkte des lokalen Netzwerks, in dem es sich befindet, übermittelt werden muss. Für diesen Fall ist ein zweiter Speicher vorgesehen, der mit den Verwaltungseinrichtungen verbunden ist, und in dem eine zweite Zuordnungstabelle zwischen den zugeordneten sekundären Kennungen und den zugeordneten tertiären Kennungen gespeichert ist. Vorzugsweise ist dieser zweite Speicher so ausgeführt, dass jede sekundäre Kennung, die von dem mobilen Endgerät für den Zugriff auf ein lokales Netzwerk verwendet wurde, aus der zweiten Tabelle gelöscht wird.

[0017] Die Erfindung bezieht sich außerdem auf eine Kommunikationsvorrichtung, die mindestens ein Haupt-Kommunikationsnetzwerk, mindestens ein drahtloses lokales Kommunikationsnetzwerk und ein Gerät oben beschriebenen Typs umfasst.

[0018] Vorzugsweise umfasst diese Vorrichtung einen Authentifizierungsserver, der den zweiten Speicher umfasst und so ausgeführt ist, dass er das Verfahren zur Authentifizierung von Kennungen beim Empfang einer tertiären Kennung und einer sekundären Kennung durch Abgleich mit den Kennungen ausführt, die in der zweiten Tabelle gespeichert sind. In diesem Fall umfasst jedes lokale Netzwerk mindestens einen Zugriffspunkt, der in der Lage ist, beim Empfang einer sekundären Kennung, die einer tertiären Kennung zugeordnet ist, dem Authentifizierungsserver einerseits eine Authentifizierungsanfrage für die empfangenen sekundären und tertiären Kennungen zu übermitteln, und andererseits dem durch die tertiäre Kennung bezeichneten mobilen Endgerät im Fall der Authentifizierung durch den Authentifizierungsserver zu ermöglichen, auf das lokale Netzwerk zuzugreifen, in dem es sich befindet.

[0019] Die Vorrichtung kann außerdem einen oder mehrere abgesicherte, private Netzwerke umfassen, die vorzugsweise mit mindestens einem der Hauptnetzwerke und mit dem Internet verbunden sind und jeweils mindestens einen Zugriffsserver sowie Verbindungseinrichtungen umfassen, die mit den Netzwerken verbunden und in der Lage sind, im Fall einer Zugriffsanforderung an ein abgesichertes, privates Netzwerk über eines der drahtlosen lokalen Netzwerke, einen gesicherten Tunnel zwischen dem privaten Netzwerk und dem lokalen Netzwerk zu erstellen.

[0020] Die Vorrichtung kann außerdem einen Fakturierungsserver umfassen, der so ausgeführt ist, dass er im Fall eines Zugriffs auf einen kostenpflichtigen Dienst von einem mobilen Endgerät über eines der drahtlosen lokalen Netzwerke die Zahlungsdaten für diesen Dienst erfasst und die diesem Dienst entsprechende Rechnung an einen Verwaltungsserver des Hauptnetzwerks übermittelt, bei dem der Nutzer des mobilen Endgeräts Kunde ist.

[0021] Im Übrigen ist jedes Netzwerk vorzugsweise über den Zugriffsserver eines Providers mit dem öffentlichen Internet verbunden.

[0022] Die Erfindung kann in zahlreichen Typen von privaten oder öffentlichen Kommunikationsnetzwerken umgesetzt werden, und insbesondere in drahtlosen lokalen Netzwerken vom Typ WLAN und Kommunikationsnetzwerken für mobile Endgeräte, die E-Mail- und Ortungsdienste bieten, insbesondere z. B. die Netze GSM, GPRS und UMTS sowie Satellitennetzwerke, wie z. B. Thuraya und Iridium.

[0023] Weitere Merkmale und Vorteile der Erfindung werden beim Durchlesen der folgenden Beschreibung und der einzigen Abbildung deutlich, in der ein Ausführungsbeispiel einer Vorrichtung gemäß der Erfindung schematisch dargestellt ist. Infolgedessen dient sie nicht nur der Ergänzung der Erfindung, sondern trägt gegebenenfalls auch zu ihrer weiteren Definition bei.

[0024] Die Kommunikationsvorrichtung gemäß der Erfindung umfasst mindestens ein Haupt-(Funk-)Kommunikationsnetzwerk RP, das einem Mobilfunkbetreiber gehört, ein öffentliches Netzwerk vom Typ INTERNET, mindestens einen Internet-Zugriffsserver **1** eines Internet-Anbieters und mindestens ein erstes drahtloses lokales Netwerk WLAN-1, das vorzugsweise mit dem Internet-Zugriffsserver **1** verbunden ist. In der Abbildung stellt das mit einer gepunkteten Linie gezeichnete Rechteck **2** sämtliche Internet-Anbieter dar.

[0025] Das Hauptnetzwerk RP ist in einem geographischen Raum angeordnet (oder installiert), wie beispielsweise einem Land, der als Hauptbereich bezeichnet wird. Es handelt sich dabei z. B. um ein Netzwerk vom Typ GSM, GPRS oder UMTS. Da diese Art von Netzwerk nicht Gegenstand der Erfindung ist und dem Fachmann bestens bekannt ist, wird sie hier nicht im Detail erläutert. Aus Gründen der Vereinfachung umfasst es eine Vielzahl von Sende- und Empfangs-Basisstationen **3**, bei einem UMTS-Netzwerk auch als Node B oder bei einem GSM-(oder GPRS-)Netzwerk als BTS bezeichnet, die jeweils einer Zelle zugeordnet werden, die einen Teil des

Hauptbereichs abdecken und direkt oder indirekt mit mehreren Arten von Endgeräten **4**, **5**, **6** verbunden sind, die auch als Knoten bezeichnet werden. Bei einem GPRS-Netzwerk handelt es sich bei diesen Knoten beispielsweise um SGSN **4** (für „Service GPRS Serving Node"), bei so genannten „2G" oder 2,5G"-Netzwerken um BSC (für „Base Station Controller") oder bei so genannten „3G"-Netzwerken um RNC (für „Radio Network Controller") **5**, die mit dem SGSN **4** verbunden sind, um GGSN **5** (für „Gateway GPRS Serving Node"), die mit SGSN **4** und dem INTERNET verbunden sind und um ein CN **6** (für „Core Network"), das mit SGSN **4** und mit mindestens einem privaten INTRANET verbunden ist, auf das im Folgenden noch näher eingegangen wird.

[0026] In dem dargestellten Beispiel ist der Knoten SGSN **4** im Übrigen auch mit einem Ortungsserver **7** verbunden, der ein Positionsmodul **8** umfasst, das dazu bestimmt ist, die Positionen der mobilen Endgeräte (oder Mobilfunk-Kommunikationsgeräte) **9** von Kunden des Hauptnetzwerks RP zu erfassen und zu speichern, sowie z. B. im Fall von GSM- und UMTS-Netzwerken ein HLR (für „Home Location Register"), das die Kundendatenbank des Hauptnetzwerks RP beinhaltet. Bei diesen mobilen Endgeräten **9** handelt es sich beispielsweise um Mobiltelefone, Laptops oder PDAs, denen primäre Kennungen zugeordnet sind, wie z. B. Telefonnummern oder E-Mail-Adressen oder eine andere Kennung, anhand der sie voneinander unterschieden werden und ihnen Meldungen adressiert werden können.

[0027] Wiederum in dem dargestellten Beispiel ist der Ortungsserver **7** zudem mit einem Diensteserver **10** vom Typ intelligentes Netzwerk (oder IN für „Intelligent Network") verbunden, der mit einem Modul für Ortungsdienste **11** ausgestattet ist, wie beispielsweise einem LBS (für „Location Based Services"). Dieser Diensteserver mit intelligentem Netzwerk **10** ist mit dem HLR verbunden und bietet die Möglichkeit, mit Hilfe einer zusätzlichen intelligenten „Schicht", die zwischen den Vermittlungsstellen/Routern und den Dienstanwendungen angeordnet ist, neue Dienste und neue Funktionalitäten in das Hauptnetzwerk RP aufzunehmen, ohne die Struktur des Hauptnetzwerks zu verändern. Das Modul für Ortungsdienste **11** dient dazu, jegliche Art von Dienst sicherzustellen, der einen Zusammenhang mit der Ortung der mobilen Endgeräte **9** der Kunden aufweist. Es arbeitet daher mit dem Ortungsserver **7** zusammen.

[0028] In einer Ausführungsvariante kann der Ortungsserver **7** entfallen, indem das Positionsmodul **8** im Diensteserver **10** angeordnet wird. Es ist auch möglich, dass das Modul für Ortungsdienste **11** (oder LBS) selbst die Funktionen zur Erfassung und Speicherung der Positionen ausführt, unabhängig vom Positionsmodul **8**. In diesem Fall sind der Diensteserver **10** und damit auch sein Modul für Ortungsdienste **11** über die herkömmlichen Mechanismen des intelligenten Netzwerks mit dem HLR und/oder dem SGSN **4** verbunden.

[0029] Dank dieses Hauptnetzwerks RP können die Kunden des Mobilfunkbetreibers Verbindungen zwischen ihren mobilen Kommunikationsendgeräten **9** und entfernten, stationären oder mobilen Kommunikationsendgeräten herstellen. Insbesondere können sie auf das INTERNET zugreifen, eventuell über den Internet-Zugangsserver **1** eines Internet-Anbieters, oder auf ein privates Netzwerk, wie beispielsweise das mit der Bezeichnung INTRANET in der Abbildung.

[0030] Natürlich existieren in einem geographischen Bereich mehrere Hauptnetzwerke nebeneinander, die verschiedenen Betreibern gehören, wobei jedes dieser Hauptnetzwerke seine eigenen Kunden hat.

[0031] Das erste drahtlose Netzwerk WLAN-i ist beispielsweise im Bereich eines Flughafens installiert (oder angeordnet), der als erster lokaler Bereich bezeichnet wird, der im Hauptbereich enthalten ist. Es handelt sich z. B. um ein Netzwerk vom Typ WLAN (für „Wireless Local Area Network"), das mit mehreren Zugriffspunkten **1** ausgerüstet ist, in die sich mobile Kommunikationsendgeräte **9** per Funk einloggen können, die mit der entsprechenden Hardware zur Verbindung mit einem lokalen Netzwerk (z. B. mit einer austauschbaren oder integrierten PC WLAN- oder einer PDA WLAN-Karte entsprechend der Norm 802.11) ausgerüstet sind. Diese Zugriffspunkte **12** sind mit einem Router (oder „Access Router") **13** verbunden, der wiederum mit dem Internet-Zugriffsserver **1** eines Internet-Anbieters verbunden ist.

[0032] In dem in der einzigen Abbildung dargestellten Beispiel umfasst die Vorrichtung ein zweites drahtloses lokales Netzwerk WLAN-2, das vorzugsweise mit dem Internet-Zugriffsserver **1** verbunden ist, sowie ein privates Netzwerk vom Typ Intranet mit der Bezeichnung INTRANET.

[0033] Das zweite drahtlose lokale Netzwerk WLAN-2 ist beispielsweise vom gleichen Typ wie das erste drahtlose lokale Netzwerk WLAN-1. Es ist beispielsweise im Bereich eines Schienennetzes mit einem Bahnhof installiert (oder angeordnet), der als zweiter lokaler Bereich bezeichnet wird, der im Hauptbereich enthalten ist. Seine Zugriffspunkte **14** sind mit einem Router (oder „Access Router") **15** verbunden, der wiederum mit dem Internet-Zugriffsserver **1** eines Internet-Anbieters verbunden ist, in diesem Fall mit dem gleichen wie beim ersten lokalen Netzwerk WLAN-1, es könnte sich jedoch auch um einen anderen Zugriffsserver handeln.

[0034] Bei dem privaten Netzwerk INTRANET han-

delt es sich beispielsweise um ein Unternehmensnetzwerk, das mit einem ersten Firewall-Server **16** für den gesicherten Zugriff auf das INTERNET, vorzugsweise vom Typ „IPsec Firewall/Gateway", sowie gegebenenfalls mit einem zweiten gesicherten Firewall-Server **17** ausgerüstet ist, der mit dem Knoten **6** des Hauptnetzwerks RP verbunden ist. Dank dieser beiden Firewall-Server **16** und **17** kann sich ein Kunde des Hauptnetzwerks RP, der für das Unternehmen tätig ist, dem das private Netzwerk INTRANET gehört, entfernt über das genannte Hauptnetzwerk in dieses Netzwerk sowie über das genannte private Netzwerk INTRANET ins INTERNET einloggen.

[0035] In dem dargestellten Beispiel sind die verschiedenen Netzwerke durch geschlossene Kurven dargestellt, die ihre jeweiligen Abdeckungsbereiche symbolisieren.

[0036] Da die Abdeckungsbereiche von INTERNET und Hauptnetzwerk RP erheblich größer sind als die der anderen Netzwerke, die sie beinhalten, wurden diese mit Strichlinien dargestellt.

[0037] Die Vorrichtung gemäß der Erfindung umfasst ein Gerät, das in dem dargestellten Beispiel dazu bestimmt ist, den Zugriff auf zwei drahtlose lokale Kommunikationsnetzwerke WLAN-1 und WLAN-2 zu kontrollieren.

[0038] Genauer gesagt ist dieses Gerät dazu bestimmt, die Erstellung von Verbindungen zwischen den mobilen Endgeräten **9** bestimmter Kunden des Hauptnetzwerks RP und dem INTERNET und/oder dem privaten Netzwerk INTRANET über eines der drahtlosen lokalen Netzwerke WLAN-i (hier i = 2) herzustellen. Auf diese Weise kann das Qualitätsniveau der vom Betreiber des Hauptnetzwerks RP angebotenen Dienste aufrechterhalten oder sogar verbessert werden, insbesondere wenn das WLAN eine höhere Bandbreite bietet als das genannte Hauptnetzwerk RP. Wie bereits erwähnt, sind von dieser Zugriffsart natürlich nur die Kunden betroffen, die über ein mobiles Kommunikationsendgerät **9** verfügen, das mit der Standardhardware für die Verbindung mit einem drahtlosen lokalen Netzwerk ausgerüstet ist (beispielsweise eine auswechselbare oder integrierte PC WLAN- oder eine PDA WLAN-Karte gemäß der Norm 802.11).

[0039] Um dieses Ziel zu erreichen, umfasst das Gerät gemäß der Erfindung vorzugsweise einen ersten Speicher **18**, in dem eine erste Zuordnungstabelle zwischen den primären Kennungen der mobilen Endgeräte **9**, die mit einem Hauptnetzwerk RP verbunden sind, und den Zugriffsberechtigungen (und/oder Zugriffsinteressen) für die drahtlosen lokalen Netzwerke WLAN-i gespeichert ist. In dieser ersten Tabelle kann eine primäre Kennung beispielsweise mehreren drahtlosen Netzwerken zugeordnet sein, wenn der entsprechende Kunde über mehrere Zugriffsberechtigungen (und/oder Interessen) verfügt, die mit dem Betreiber des Hauptnetzwerks RP vereinbart wurden. Wie bereits erläutert, bezeichnet diese primäre Kennung nicht zwangsläufig das mobile Endgerät, das sich in ein drahtloses lokales Netzwerk einwählen kann. Dies kann der Fall sein, es kann jedoch auch ein erstes mobiles Endgerät vom Typ Mobiltelefon bezeichnen, das einem Kunden gehört, der über ein zweites mobiles Endgerät verfügt, mit dem die genannte Verbindung hergestellt werden kann, wie z. B. ein PDA oder einen PC.

[0040] Wenn mehrere Betreiber nebeneinander existieren, was im Allgemeinen der Fall ist, sieht man für jedes Betreiber-Hauptnetzwerk einen ersten Speicher **18** vor. Dieser wird dann vorzugsweise in einem Server des Betreibers angeordnet, beispielsweise dem Diensteserver **10**, wie in der Abbildung dargestellt. Man kann auch eine Kopie jeder ersten Tabelle in einem Server **19** speichern, z. B. vom Typ AAA (für „Autorisation, Authentication, Accounting"), die von den verschiedenen Internet-Anbietern gemeinsam genutzt wird. Das Gerät gemäß der Erfindung umfasst im Wesentlichen ein Verwaltungsmodul **20**, das mit dem Positionsmodul **8**, dem Modul für Ortungsdienste **11** und mit dem ersten Speicher **18**, sofern vorhanden, verbunden ist.

[0041] Dieses Verwaltungsmodul **20** ist vorzugsweise im Diensteserver **10** des Betreibers angeordnet. Es könnte jedoch auch in einem anderen Server des Betreibers angeordnet werden, wie beispielsweise im Ortungsserver **7**. Genauer gesagt ist es vorzuziehen, es im gleichen Server anzuordnen, in dem sich auch der erste Speicher **18** befindet. Es ist dazu bestimmt, mehrere Schritte auszuführen.

[0042] Ein erster Schritt besteht darin, die Positionen der mobilen Endgeräte **9**, die als für die Verbindung mit drahtlosen lokalen Netzwerken WLAN-i geeignet registriert wurden oder einem anderen mobilen Kommunikationsendgerät zugeordnet sind, das für diese Art von Verbindung geeignet ist, die vom Positionsmodul **8** an den Ortungsserver **7** übertragen werden, mit den Positionen des ersten und zweiten lokalen Bereichs zu vergleichen, um diejenigen auszuwählen, die sich ungefähr in einem der lokalen Bereiche oder in seiner unmittelbaren Umgebung befinden.

[0043] Ein zweiter Schritt besteht darin, Anweisungen an ein Modul zu adressieren, das die Aufgabe hat, Ortungsmitteilungen innerhalb des Hauptnetzwerks RP zu übermitteln, dem die ausgewählten mobilen Endgeräte zugeordnet sind, wobei diese Anweisungen zumindest ihre primäre Kennung und einen Code umfassen, der es veranlasst, jedem durch eine der empfangenen primären Kennungen bezeichneten mobilen Endgeräte **9** über das Hauptnetzwerk RP

eine Meldung zu adressieren, in der seinem Nutzer mitgeteilt wird, dass er sich in das drahtlose lokale Netzwerk WLAN-i einloggen kann, in dem er sich derzeit aufhält oder in einen dessen lokaler Bereiche er sich gerade begibt. Bei diesem Modul handelt es sich vorzugsweise um das Modul für Ortungsdienste **11**, das im intelligenten Diensteserver **10** angeordnet ist, insbesondere wenn es sich um ein Modul **11** vom Typ LBS handelt.

[0044] Wenn es sich um ein Modul **11** vom Typ LBS handelt, das mit dem HLR verbunden ist, das die Datenbank mit den Kunden des Hauptnetzwerks RP enthält, kann man in Betracht ziehen, dass das Verwaltungsmodul **20** ihm alle primären Kennungen der erfassten mobilen Endgeräte übermittelt, so dass es nur an die mobilen Endgeräte Meldungen überträgt, die einer in einer Liste eingetragenen primären Kennung zugeordnet sind, die in einem Speicher oder in der ersten Tabelle gespeichert ist, beispielsweise entsprechend einer Zugriffsberechtigung für ein WLAN.

[0045] Wenn man eine erste Zuordnungstabelle vorsieht, ist das Verwaltungsmodul **20** vorzugsweise so ausgeführt, dass es zwischen dem ersten und dem zweiten Schritt einen dritten Schritt durchführen kann. Dieser dritte Schritt besteht darin, auf die erste Zuordnungstabelle zuzugreifen, die im Speicher **18** gespeichert ist, um aus den ausgewählten mobilen Endgeräten **9** diejenigen zu ermitteln, die für den lokalen Bereich, in dem sie sich aufhalten, über eine Zugriffsberechtigung (und/oder ein Zugriffsinteresse) für das lokale Netzwerk verfügen. Diese Ermittlung erfolgt ausgehend von den primären Kennungen, die den mobilen Endgeräten **9** zugeordnet sind. Infolgedessen handelt es sich um die primären Kennungen, die man bei dieser Ermittlung erfasst (oder auswählt). In diesem Fall werden nur den mobilen Endgeräten Meldungen übermittelt, deren primäre Kennungen ausgewählt wurden.

[0046] Beim Empfang der Anweisung generiert das Modul für Lokalisierungsdienste **11** eine spezifische Meldung für jedes erfasste oder ausgewählte mobile Endgerät **9**. Vorzugsweise sind diese Meldungen vom Typ SMS (für „Short Messaging System"), es kann sich jedoch auch um E-Mails handeln.

[0047] Wenn ein Kunde auf seinem mobilen Endgerät **9** eine Meldung empfängt, kann er versuchen, sich in das drahtlose lokale Netzwerk WLAN-i in dem lokalen Bereich, in dem er sich aufhält, einzuloggen, entweder um netzwerkinterne Informationen abzurufen oder um sich ins INTERNET oder auch in sein Unternehmensnetzwerk INTRANET einzuloggen.

[0048] Es können zwei Fälle auftreten, je nachdem, ob das mobile Endgerät **9** tatsächlich für die Verbindung mit dem WLAN-i geeignet ist oder ob es für diese Art von Verbindung nicht geeignet ist, jedoch einem Kunden gehört, der außerdem ein PDA oder einen Laptop besitzt, der für diese Art von Verbindung ausgerüstet ist. Im zuletzt genannten Fall empfängt der Kunde auf seinem „herkömmlichen" Mobiltelefon **9** die vom Hauptnetzwerk RP versandte Meldung (SMS) und muss versuchen, mit seinem entsprechend ausgerüsteten PDA oder seinem Laptop **9** eine Verbindung herzustellen.

[0049] Es ist nicht unbedingt erforderlich, dass sich das erfasste mobile Endgerät **9** innerhalb eines lokalen Bereichs befindet. Man kann nämlich vorsehen, dass der Erfassungsschritt den Begriff eines Entfernungsgrenzwerts beinhaltet. Wenn sich also das mobile Endgerät in einem bestimmten Abstand zur Grenze eines lokalen Bereichs befindet, der unter dem Entfernungsgrenzwert liegt, kann man ihm eine Meldung übermitteln. Auf diese Weise ist es insbesondere möglich, ihn zu benachrichtigen, dass er dabei ist, in einen lokalen Bereich zu gelangen oder dass er sich in der Nähe eines lokalen Bereichs aufhält, in dem er versuchen könnte, sich in das entsprechende drahtlose lokale Netzwerk einzuloggen. Somit kann sich ein Kunde dank der Erfindung in den nächstgelegenen lokalen Bereich begeben, um eine Verbindung herzustellen, die er außerhalb dieses Bereichs nicht herstellen kann. Daher kann man vorsehen, dass die Meldung eine Information über den Abstand beinhaltet, der das mobile Endgerät **9** von der Grenze eines lokalen Bereichs trennt. Infolgedessen kann man vorsehen, dass die Meldung Informationen umfasst, die dem Nutzer ermöglichen, den benachbarten lokalen Bereich zu finden, dessen Vorhandensein ihm mitgeteilt wird.

[0050] Die Verbindung des mobilen Endgeräts **9** des Kunden mit dem drahtlosen lokalen Netzwerk WLAN-i erfolgt über den nächsten Zugriffspunkt **12** oder **14**. Der Zugriffspunkt **12** oder **14** überträgt dann eine Empfangsseite vom Typ „Web" an das mobile Endgerät **9**, damit es die internen Informationen des drahtlosen lokalen Netzwerks WLAN-i nutzen und/oder sich über den Internet-Zugriffsserver **1**, mit dem der Router **13** des drahtlosen lokalen Netzwerks WLAN-i verbunden ist, ins INTERNET oder ein INTRANET einloggen kann.

[0051] Vorzugsweise erfolgt die Verbindung mit dem INTERNET oder einem INTERNET auf gesicherte Weise. Zu diesem Zweck kann man in die Meldungen an die ausgewählten (oder erfassten) mobilen Endgeräte eine sekundäre Kennung integrieren, wie z. B. ein alphanumerisches Passwort.

[0052] Dieses Passwort wird vorzugsweise vom Verwaltungsmodul **20** zugeordnet und ergibt sich beispielsweise aus einer zufälligen Auswahl. In diesem Fall wird dem Modul für Ortungsdienste **11** die sekundäre Kennung mit den anderen Anweisungen zur

Meldungserzeugung adressiert. Diese sekundäre Kennung ist vorzugsweise in einer zweiten Zuordnungstabelle für eine tertiäre Kennung gespeichert, bei der es sich um einen Benutzernamen oder ein primäre Kennung handeln kann. Diese zweite Tabelle ist z. B. im ersten Speicher **18** gespeichert. Aus Gründen der schnelleren Verarbeitung ist es ebenfalls zu bevorzugen, dass eine Kopie der zweiten Tabellen für die verschiedenen Betreiber in einem zweiten Speicher **21** des Servers **19** gespeichert ist, den die verschiedenen Internet-Anbieter gemeinsam nutzen. Dies ist insbesondere interessant, wenn der genannte Server **19** vom Typ AAA ist, da ein solcher Server insbesondere dazu konzipiert ist, Authentifizierungsverfahren auszuführen. In diesem Fall, um die Übertragung der zweiten Zuordnungstabellen vom Hauptnetzwerk an den Server **19** vom Typ AAA zu ermöglichen, ist ein Server **22** vorgesehen, z. B. vom Typ „Proxy", der vorzugsweise mit dem Knoten GGSN **5** jedes Hauptnetzwerks RP und dem genannten Server **19** vom Typ AAA verbunden ist. Wird ein Authentifizierungsverfahren eingeleitet, müssen die Zugriffspunkte **12** und **14** der drahtlosen lokalen Netzwerke WLAN-i entsprechend angepasst werden, um eine Empfangsseite an die mobilen Endgeräte **9** zu übertragen, die den Nutzer auffordert, die sekundäre Kennung einzugeben, die er von seinem Hauptnetzwerk RP erhalten hat, sowie gegebenenfalls seinen Nutzernamen (tertiäre Kennung). Bestimmte Zugriffspunkte, wie z. B. die von der Firma COLUBRIS gelieferten, sind für diese Zwecke ausgerüstet.

[0053] Sobald er die sekundäre und tertiäre Kennung erfasst hat, sendet der Zugriffspunkt **12** oder **14** eine Authentifizierungsanfrage über den Router **13** oder **15** an den Server **19** vom Typ AAA. Diese Anfrage wird vorzugsweise in Form einer Internet-Seite übertragen, auf der die vom Nutzer eingegebenen Kennungen eingegeben werden. Sie wird vorzugsweise entsprechend dem gesicherten Protokoll HTTPS (für „HyperText Transfer Protocol Secure") übertragen. Beim Empfang dieser Anfrage liest das Authentifizierungsmodul die darin enthaltene sekundäre und tertiäre Kennung aus und vergleicht diese mit den in der zweiten Tabelle des zweiten Speichers **21** abgelegten Angaben. Wenn das Authentifizierungsmodul sein Authentifizierungsverfahren beendet hat, generiert es eine Meldung zur Freigabe oder Sperrung der Verbindung.

[0054] Im Fall einer Freigabe gibt der betreffende Zugriffspunkt **12** oder **14** den Zugriff auf die für das mobile Endgerät **9** verfügbaren Dienste frei. Wenn der Nutzer dem Zugriffspunkt eine Zugriffsanfrage für das INTERNET übermittelt, erhält sein mobiles Endgerät **9** die Verbindung über den Router **13** oder **15** des WLAN-i und über den Zugriffsserver **1**, mit dem der genannte Router verbunden ist, aufrecht. Wenn der Nutzer dem Zugriffspunkt eine Anfrage für den Zugriff auf ein privates Netzwerk übermittelt, wie z. B. das Unternehmensnetzwerk INTRANET, wird vorzugsweise zunächst eine gesicherte Verbindung (oder ein gesicherter Tunnel) zwischen dem WLAN-i und dem Firewall-Server **16** vom Typ Firewall/Gateway des INTRANETs über das INTERNET hergestellt. Dieser gesicherte Tunnel nutzt vorzugsweise ein gesichertes Internet-Protokoll für ein virtuelles privates Netzwerk (oder VPN für „Virtual Private Network") vom Typ „IPsec", das für die Verbindung von entfernten, privaten Netzwerken mit einem öffentlichen IP-Netzwerk geeignet ist. Natürlich muss der Firewall-Server **16** mit diesem gesicherten Protokolltyp kompatibel sein.

[0055] Die sekundären Kennungen sollten vorzugsweise „zum einmaligen Gebrauch" sein, so dass sie nur eine einmalige Verbindung eines mobilen Endgeräts **9** mit einem drahtlosen lokalen Netzwerk WLAN-i ermöglichen. Um diese Funktionalität zu implementieren, können mindestens vier Lösungen umgesetzt werden. Eine erste Lösung besteht darin, das Paar (sekundäre Kennung, tertiäre Kennung) aus der zweiten Tabelle zu löschen, sobald die Freigabe für die entsprechende Verbindung erteilt wurde. Eine zweite Lösung besteht darin abzuwarten, bis das mobile Endgerät **9** die Verbindung mit einem Zugriffspunkt **12** oder **14** unterbricht, um dem Server **19**, in dem der zweite Speicher **21** vorzugsweise angeordnet ist, eine Anfrage zum Löschen des diesem Endgerät zugeordneten Paars zu übermitteln. Die Trennung der Verbindung kann durch Beobachtung des Verkehrs erfasst werden. Ist beispielsweise kein Verkehr mehr vorhanden, kann ein „Time-Out" durchgeführt werden. Eine dritte Lösung besteht darin, den Zugriff für ein WLAN für eine bestimmte, wählbare Zeitdauer freizugeben, beispielsweise eine Stunde, unabhängig von der Anzahl an Verbindungen. In diesem Fall erfolgt der Befehl zum Löschen des Paars im zweiten Speicher **21**, wenn die genannte Zeitdauer abgelaufen ist. Eine vierte Lösung besteht darin, das Paar im zweiten Speicher **21** zu löschen, wenn eine bestimmte Datenmenge übertragen wurde, unabhängig von der Anzahl an Verbindungen.

[0056] Mit Hilfe dieses Verbindungstyps über ein WLAN kann der Kunde eines Mobilfunkbetreibers insbesondere E-Mails versenden oder auf sein Postfach zugreifen, um die erhaltenen E-Mails abzurufen oder auf private Informationen zuzugreifen, ohne über das Hauptnetzwerk RP seines Betreibers zu gehen.

[0057] Wenn der Nutzer über das WLAN auf kostenpflichtige Dienste zugreift, erfolgt die Erfassung der Informationen zur Dienstefakturierung über ein Erfassungsmodul, das vorzugsweise im gemeinsamen Server **19** der Internet-Anbieter angeordnet ist. Dies ist insbesondere interessant, wenn der genannte Server **19** vom Typ AAA ist, weil dieser über ein solches Erfassungsmodul verfügt.

[0058] Sobald die Fakturierungsinformationen erfasst wurden, werden sie an den Betreiber weitergeleitet, dessen Kunde der Nutzer ist.

[0059] Das Verwaltungsmodul **20** kann in Form von elektronischen Schaltungen, Software-Modulen (oder EDV-Modulen) oder als Kombination aus Schaltungen und Software ausgeführt werden.

[0060] In einer Vorrichtung gemäß der Erfindung kann man vorsehen, dass jeder Betreiber mit einem derartigen Gerät ausgerüstet ist oder dass alle Betreiber ein gemeinsames Gerät nutzen. Unter „Gerät" versteht man in der vorliegenden Beschreibung mindestens ein Verwaltungsmodul, das mit der ersten Tabelle und einem Positionsmodul **8** verbunden werden kann, das die nominalen Positionen der mobilen Kommunikationsendgeräte **9** der Kunden eines Hauptnetzwerks RP erfassen und speichern kann, und beispielsweise in einem Ortungsserver vom Typ HLR angeordnet ist, sowie mit einem Modul für Ortungsdienste **11**, wie z. B. einem LBS, das beispielsweise in einem Diensteserver **10** vom Typ intelligentes Netzwerk angeordnet ist. Das Gerät kann außerdem eine erste Zuordnungstabelle zwischen primären Kennungen und Zugriffsberechtigungen für drahtlose lokale Netzwerke umfassen, die in einem ersten Speicher **18** gespeichert ist, und/oder eine zweite Zuordnungstabelle zwischen sekundären Kennungen und tertiären Kennungen, die in einem zweiten Speicher **21** gespeichert ist.

[0061] Im Übrigen wird in diesem Verfahren auf mobile Endgeräte Bezug genommen, die einem Nutzer gehören, der Kunde des Betreibers eines Hauptnetzwerks RP ist. Es ist jedoch auch vorstellbar, dass bestimmte mobile Endgeräte Nutzern gehören, die nicht Kunden eines Betreibers sind, und die aus diesem Grund nicht vom Betreiber eines Hauptnetzwerks RP geortet werden können. Um diesen Personen die Möglichkeit zu bieten, sich in dem lokalen Bereich, in dem sie sich aufhalten, in ein drahtloses lokales Netzwerk WLAN-i einzuloggen, sind zwei Lösungen denkbar.

[0062] Eine erste Lösung besteht darin, den potenziellen Nutzern, vorzugsweise an Verkaufspunkten in den betreffenden lokalen Bereichen (dies ist jedoch auch an jedem anderen Ort möglich), kostenpflichtige Rubbelkarten (oder „Scratch Cards") anzubieten, die eine sekundäre Kennung, wie beispielsweise ein alphanumerisches Passwort sowie eventuell einen Benutzernamen enthalten.

[0063] Eine zweite Lösung besteht darin, einen Sprachserver vorzusehen, der beispielsweise über eine öffentliche Telefonzelle zugänglich ist, in dem eine bestimmte kostenpflichtige Rufnummer (vom Typ 0836...) gewählt wird. Sobald die Verbindung mit dem Sprachserver hergestellt wurde, sagt dieser dem Anrufer eine sekundäre Kennung, wie z. B. ein alphanumerisches Passwort sowie gegebenenfalls einen Benutzernamen an.

[0064] Bei diesen beiden Lösungen kann sich der genannte Nutzer, sobald er im Besitz seines Passworts (sowie gegebenenfalls seines Benutzernamens) ist, mit Hilfe seines mobilen Endgeräts, das mit geeigneten Verbindungseinrichtungen ausgerüstet ist, von einem Zugriffspunkt **12** oder **14** des WLAN-i in dem lokalen Bereich, in dem er sich befindet, einloggen. Die sekundären Kennungen (und Benutzernamen), die auf den kostenpflichtigen Karten aufgedruckt sind oder von dem Sprachserver telefonisch mitgeteilt werden, sind in zweiten Speicher **21** des Servers **19** gespeichert, so dass das Authentifizierungsverfahren ausgeführt werden kann. Die Funktionsweise ist anschließend identisch mit der oben beschriebenen, außer dass der Zugriff auf das Internet und/oder ein Intranet über WLAN-i oder einfach auf das WLAN-i keine Fakturierung zur Folge hat und nur kostenlose Dienste betrifft.

[0065] Die Erfindung bietet zudem ein Verfahren für die Zugriffskontrolle auf ein oder mehrere drahtlose lokale Kommunikationsnetzwerke (vom Typ WLAN), die jeweils einen lokalen Abdeckungsbereich aufweisen, der zumindest teilweise im Hauptabdeckungsbereich eines oder mehrerer Haupt-Kommunikationsnetzwerke enthalten ist.

[0066] Dieses kann mit Hilfe des oben beschriebenen Geräts und der Vorrichtung umgesetzt werden. Da die hauptsächlichen und optionalen Funktionen und Unterfunktionen, die durch die Schritte dieses Verfahrens gewährleistet werden, in etwa identisch sind wie diejenigen, die von den verschiedenen Komponenten des Geräts und der Vorrichtung gewährleistet werden, werden im Folgenden nur die Schritte erläutert, in denen die wesentlichen Funktionen des Verfahrens gemäß der Erfindung umgesetzt werden. Dieses Verfahren umfasst:

– zunächst die Erfassung der Position zumindest bestimmter mobiler Kommunikationsendgeräte, die Kunden eines Hauptnetzwerks gehören, die sich im Hauptbereich aufhalten, anschließend
– den Vergleich dieser Positionen mit denen lokaler Bereiche, um die primären Kennungen der mobilen Endgeräte auszuwählen, die sich ungefähr in einem der lokalen Bereich befinden, und
– Adressierung einer Meldung über das Hauptnetzwerk an jedes ausgewählte mobile Endgerät, in der dem Nutzer mitgeteilt wird, dass er sich in dem lokalen Bereich, in dem er sich aufhält, in ein lokales Netzwerk einloggen kann.

[0067] Die Verbindung kann dann entweder direkt oder nach einem Schritt zur Authentifizierung hergestellt werden. In letzterem Fall beinhalten die Meldungen an die mobilen Endgeräte zudem eine sekundäre

Kennung, vorzugsweise für den einmaligen Gebrauch.

[0068] Man kann außerdem einen zusätzlichen Schritt nach der Phase zur Auswahl der primären Kennung(en) vorsehen, der darin besteht, auf eine erste Zuordnungstabelle zwischen den primären Kennungen der mobilen Endgeräte und Zugriffsberechtigungen für lokale Netzwerk zuzugreifen, um diejenigen auszuwählen, die über eine Zugriffsberechtigung (oder ein Zugriffsinteresse) für das lokale Netzwerk in dem lokalen Bereich verfügen, in dem sich das entsprechende mobile Endgerät befindet. In diesem Fall werden nur Meldungen an die mobilen Endgeräte gesandt, deren primäre Kennungen ausgewählt wurden.

[0069] Die Erfindung bezieht sich auf alle öffentlichen Mobilfunk-Hauptnetzwerke, die Dienste für Mitteilungen und Ortung anbieten, und insbesondere auf Netzwerke vom Typ GSM, GPRS und UMTS, das Internet (IP), alle privaten Netzwerke sowie alle drahtlosen lokalen Netzwerke, insbesondere diejenigen vom Typ WLAN. Sie bezieht sich jedoch ebenfalls auf Satellitennetzwerke, wie z. B. Thuraya und Iridium.

[0070] Die Erfindung ist nicht auf die vorstehend beschriebenen Ausführungsvarianten des Verfahrens, der Vorrichtung und des Geräts beschränkt, die lediglich Beispielcharakter haben, sondern umfasst alle Varianten, die der Fachmann im Rahmen der folgenden Ansprüche umsetzen könnte.

Patentansprüche

1. Zugriffskontrollverfahren für mindestens ein drahtloses lokales Netzwerk mit einem lokalen Abdeckungsbereich, der zumindest teilweise im Hauptabdeckungsbereich mindestens eines Haupt-Kommunikationsnetzwerks enthalten ist, wobei dieses Verfahren die folgenden Schritte umfasst:
i) Ermittlung der Position zumindest bestimmter mobiler Kommunikationsendgeräte (**9**), die Kunden des Hauptnetzwerks gehören, die sich im Hauptbereich aufhalten,
ii) Vergleich der genannten Positionen zumindest einiger der genannten mobilen Endgeräte (**9**) in den Verwaltungseinrichtungen (**20**) des Hauptnetzwerks mit der Position mindestens eines lokalen Bereichs zur Auswahl der primären Kennungen der mobilen Endgeräte, die sich in dem genannten lokalen Bereich befinden oder die sich in einem bestimmten Abstand zur Grenze des genannten lokalen Bereichs aufhalten, wobei dieser Abstand unter einem vorab definierten Entfernungsgrenzwert liegt,
dadurch gekennzeichnet, dass
iii) Anweisungen an einen E-Mail-Server (**10**) des Hauptnetzwerks adressiert werden, die mindestens die primäre Kennung jedes ausgewählten mobilen Endgeräts (**9**) beinhalten, so dass er automatisch eine Meldung an jedes der genannten mobilen Endgeräte sendet, in der seinem Nutzer mitgeteilt wird, dass er sich im lokalen Bereich eines lokalen Netzes aufhält, in das er sich einloggen kann.

2. Verfahren gemäß Anspruch 1, dadurch gekennzeichnet, dass die Adressierung einer Meldung an ein mobiles Endgerät (**9**), das erfasst wurde, nach der Auswahl der primären Kennungen außerdem Folgendes umfasst:
– Zugriff auf eine erste Zuordnungstabelle zwischen den primären Kennungen der mobilen Endgeräte und Zugriffsberechtigungen für ein lokales Netzwerk, so dass aus den ausgewählten primären Kennungen diejenigen ermittelt werden können, denen eine Zugriffsberechtigung für das genannte lokale Netzwerk zugeordnet ist, und anschließend
– Adressierung von Meldungen an die mobilen Endgeräte (**9**), deren primäre Kennungen ausgewählt wurden.

3. Verfahren gemäß Anspruch 1, dadurch gekennzeichnet, dass jede Meldung eine eigene sekundäre Kennung umfasst, sowie dadurch, dass der Nutzer eines ausgewählten oder erfassten mobilen Endgeräts im Fall eines Verbindungsversuchs mit dem lokalen Netzwerk die empfangene sekundäre Kennung eingeben muss.

4. Verfahren gemäß Anspruch 3, dadurch gekennzeichnet, dass man beim Empfang einer sekundären Kennung, die einer tertiären Kennung zugeordnet ist, über das genannte lokale Netzwerk auf eine zweite Zuordnungstabelle zwischen sekundären Kennungen und tertiären Kennungen zugreift, um die genannte Verbindung zu authentifizieren, und dass im Fall der Authentifizierung dem mobilen Endgerät (**9**) ermöglicht wird, auf das genannte lokale Netzwerk zuzugreifen.

5. Verfahren gemäß Anspruch 3, dadurch gekennzeichnet, dass die sekundäre Kennung für den einmaligen Gebrauch bestimmt ist.

6. Verfahren gemäß Anspruch 1, dadurch gekennzeichnet, dass die genannten Meldungen entsprechend dem Modus „Short Messaging System" adressiert werden.

7. Verfahren gemäß Anspruch 1, dadurch gekennzeichnet, dass im Fall eines Zugriffs auf ein gesichertes privates Netzwerk über das genannte lokale Netzwerk eine Verbindung mit dem genannten privaten und lokalen Netzwerk über einen gesicherten Tunnel hergestellt wird.

8. Verfahren gemäß Anspruch 1, dadurch gekennzeichnet, dass im Fall eines Zugriffs auf einen kostenpflichtigen Dienst über das genannte lokale Netzwerk eine Erfassung der Zahlungsdaten für den

genannten Dienst im Hinblick auf die Fakturierung des genannten Dienstes über das genannte Hauptnetzwerk durchgeführt wird, dem das genannte mobile Endgerät (**9**) zugeordnet ist, das auf den genannten Dienst zugegriffen hat.

9. Gerät zur Zugriffskontrolle auf mindestens ein drahtloses lokales Kommunikationsnetzwerk mit einem lokalen Abdeckungsbereich, der zumindest teilweise in dem Hauptabdeckungsbereich mindestens eines Haupt-Kommunikationsnetzwerks enthalten ist, das mit Positionseinrichtungen für mobile Kommunikationsendgeräte (**9**) ausgerüstet ist und Verwaltungseinrichtungen (**20**) umfasst, die mit den genannten Positionseinrichtungen (**8**) verbunden und entsprechend ausgeführt sind, um
i) die Position zumindest bestimmter der genannten mobilen Endgeräte (**9**) mit der Position mindestens eines lokalen Bereichs zu vergleichen, um die primären Kennungen der mobilen Endgeräte auszuwählen, die sich in dem genannten lokalen Bereich befinden oder in einem bestimmten Abstand zur Grenze des genannten lokalen Bereichs angeordnet sind, wobei dieser Abstand unter einem vorher definierten Entfernungsgrenzwert liegt, und dadurch gekennzeichnet, dass es Verwaltungseinrichtungen umfasst, die entsprechend ausgeführt sind, um
ii) an einen E-Mail-Server (**10**) des Hauptnetzwerks Anweisungen zu adressieren, die mindestens eine primäre Kennung jedes ausgewählten mobilen Endgeräts (**9**) beinhalten, so dass an jedes der genannten mobilen Endgeräte automatisch eine Meldung gesandt wird, in der seinem Nutzer mitgeteilt wird, dass er sich im lokalen Bereich eines lokalen Netzwerks aufhält, in das er sich einloggen kann.

10. Gerät gemäß Anspruch 9, dadurch gekennzeichnet, dass es einen ersten Speicher (**18**) umfasst, in dem eine erste Zuordnungstabelle zwischen den primären Kennungen der mobilen Endgeräte (**9**) und Zugriffsberechtigungen für ein lokalen Netzwerk gespeichert ist, sowie dadurch, dass das genannte Verwaltungsmodul (**20**) mit dem ersten Speicher (**18**) verbunden und entsprechend ausgeführt ist, um auf die erste Zuordnungstabelle zuzugreifen, um aus den ausgewählten primären Kennungen diejenigen zu erfassen, die über eine Zugriffsberechtigung für das lokale Netzwerk in dem lokalen Bereich verfügen, in dem sich das entsprechende mobile Endgerät befindet.

11. Gerät gemäß Anspruch 9, dadurch gekennzeichnet, dass die genannten Verwaltungseinrichtungen (**20**) entsprechend ausgeführt sind, um dem genannten E-Mail-Server (**10**) Anweisungen zu adressieren, die eine sekundäre Kennung enthalten, die jedem ausgewählten mobilen Endgerät (**9**) speziell zugeordnet ist, wobei die genannte sekundäre Kennung von dem entsprechenden mobilen Endgerät an einem der Zugriffspunkte (**12**, **14**) des lokalen Netzwerks bei einem Verbindungsversuch mit dem genannten lokalen Netzwerk angegeben werden muss.

12. Gerät gemäß Anspruch 11, dadurch gekennzeichnet, dass es einen zweiten Speicher (**21**) umfasst, der von den genannten Verwaltungseinrichtungen (**20**) genutzt wird und entsprechend ausgeführt ist, um eine zweite Zuordnungstabelle zwischen den zugeordneten sekundären Kennungen und den zugeordneten tertiären Kennungen zu speichern, wobei Letztere zusammen mit der entsprechenden sekundären Kennung angegeben werden muss.

13. Gerät gemäß Anspruch 12, dadurch gekennzeichnet, dass der genannte zweite Speicher (**21**) entsprechend ausgeführt ist, um die genannte zweite Tabelle zu löschen, wobei jede sekundäre Kennung von einem mobilen Endgerät (**9**) für den Zugriff auf das genannte lokale Netzwerk verwendet wurde.

14. Gerät gemäß Anspruch 9, dadurch gekennzeichnet, dass die genannten Verwaltungseinrichtungen (**20**) entsprechend ausgeführt sind, um den Zugriff auf mindestens zwei unabhängige lokale Netzwerke zu kontrollieren.

15. Kommunikationsvorrichtung mit mindestens einem Haupt-Kommunikationsnetzwerk und mindestens einem drahtlosen lokalen Kommunikationsnetzwerk, dadurch gekennzeichnet, dass sie außerdem ein Gerät gemäß einem der Ansprüche 9 bis 14 umfasst.

16. Vorrichtung gemäß Anspruch 15, dadurch gekennzeichnet, dass sie einen Authentifizierungsserver (**19**) umfasst, der den genannten zweiten Speicher (**21**) umfasst und entsprechend ausgeführt ist, um beim Empfang einer tertiären Kennung und einer sekundären Kennung ein Authentifizierungsverfahren für die Kennungen auszuführen, indem diese mit den in der zweiten Tabelle gespeicherten Kennungen verglichen werden, sowie dadurch, dass jedes lokale Netzwerk mindestens einen Zugriffspunkt (**12**, **14**) umfasst, der entsprechend ausgeführt ist, um beim Empfang einer sekundären Kennung, die einer tertiären Kennung zugeordnet ist, Folgendes auszuführen:
– Adressierung einer Authentifizierungsanfrage für die empfangene sekundäre und tertiäre Kennung an den genannten Authentifizierungsserver (**19**), und
– im Fall der Authentifizierung durch den genannten Authentifizierungsserver (**19**), Freigabe für das von der tertiären Kennung bezeichnete mobile Endgerät (**9**), auf das lokale Netzwerk, in dem es sich befindet, zuzugreifen.

17. Vorrichtung gemäß Anspruch 15, dadurch gekennzeichnet, dass sie zudem mindestens ein gesichertes privates Netzwerk, das mindestens einen Zugriffsserver (**16**, **17**) umfasst, der mit mindestens einem der genannten Hauptnetzwerke verbunden ist,

sowie Verbindungseinrichtungen umfasst, die mit den genannten Netzwerken verbunden und in der Lage sind, im Fall einer Zugriffsanforderung für ein gesichertes privates Netzwerk über eines der genannten lokalen Netzwerke einen gesicherten Tunnel zwischen dem genannten privaten Netzwerk und dem genannten lokalen Netzwerk zu erstellen.

18. Vorrichtung gemäß Anspruch 17, dadurch gekennzeichnet, dass das genannte private Netzwerk mit einem öffentlichen Netzwerk verbunden ist.

19. Vorrichtung gemäß Anspruch 15, dadurch gekennzeichnet, dass sie einen Fakturierungsserver (**19**) umfasst, der entsprechend ausgeführt ist, um im Fall des Zugriffs eines mobilen Endgeräts (**9**) über eines der genannten lokalen Netzwerke auf einen kostenpflichtigen Dienst die Zahlungsdaten in Bezug auf den genannten Dienst zu erfassen und eine dem genannten Dienst entsprechende Rechnung an einen Verwaltungsserver (**10**) des Hauptnetzwerks zu übermitteln, dessen Kunde der Nutzer des genannten mobilen Endgeräts ist.

20. Vorrichtung gemäß Anspruch 15, dadurch gekennzeichnet, dass das genannte lokale Netzwerk über einen Zugriffsserver eines Internet-Anbieters (**1**) mit dem öffentlichen Netzwerk verbunden ist.

21. Vorrichtung gemäß Anspruch 15, dadurch gekennzeichnet, dass das genannte Hauptnetzwerk mit dem öffentlichen Netzwerk verbunden ist.

22. Umsetzung des Verfahrens, des Geräts und der Vorrichtung gemäß einem der vorgenannten Ansprüche in Netzwerken aus einer Gruppe, die öffentliche Kommunikationsnetzwerke für mobile Endgeräte, die E-Mail- und Ortungsdienste anbieten, drahtlose lokale Netzwerke vom Typ WLAN und Satellitennetzwerke umfassen.

23. Umsetzung des Verfahrens gemäß Anspruch 22, dadurch gekennzeichnet, dass die PLMN-Netzwerke GSM-, GPRS- und UMTS-Netzwerke umfassen.

Es folgt ein Blatt Zeichnungen

Anhängende Zeichnungen