

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
23. Juli 2020 (23.07.2020)



(10) Internationale Veröffentlichungsnummer
WO 2020/148039 A1

(51) Internationale Patentklassifikation:

H04L 29/06 (2006.01) H04W 48/04 (2009.01)
H04W 12/08 (2009.01)

(21) Internationales Aktenzeichen: PCT/EP2019/085154

(22) Internationales Anmeldedatum:
13. Dezember 2019 (13.12.2019)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2019 200 409.1
15. Januar 2019 (15.01.2019) DE

(71) Anmelder: OSRAM GMBH [DE/DE]; Marcel-Breuer-Straße 6, 80807 München (DE).

(72) Erfinder: SACHER, Holger; Am Gruenland 81, 86169 Augsburg (DE). JUNG, Markus; Wendelsteinstraße 12, 85622 Feldkirchen (DE). ESCHEY, Michael; Am Hofacker 16, 86517 Wehringen (DE). ERNST, Herbert; Kiefernstr. 4, 82362 Weilheim (DE).

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(54) Title: SYSTEM FOR PROVIDING A WIRELESS NETWORK

(54) Bezeichnung: SYSTEM ZUM BEREITSTELLEN EINES DRAHTLOSEN NETZWERKS

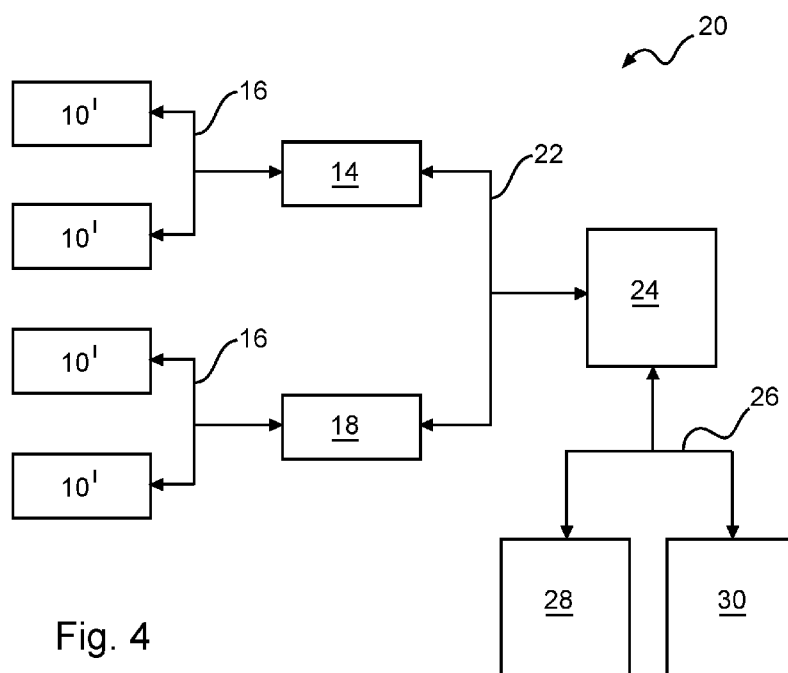


Fig. 4

(57) Abstract: The invention relates to a system (20) for providing a wireless network, the system comprising a plurality of wireless access points (10, 10'), each of which provides access to the wireless network for a delimited spatial area in a building (1, 1') or in a physical structure. At least one spatial zone controller (14, 18) is also provided which is connected to at least some of the wireless access points and is designed to receive, via the wireless access points connected to said controller, device information regarding a terminal (32) logging into the network and/or regarding an external wireless access point, and to determine the spatial position of the terminal (32) in question and/or of the external wireless access point in or close to the building (1) or the physical structure on the basis of an association with one or more of the connected wireless access points. In addition, a central security controller (24) is provided which is



(84) **Bestimmungsstaaten** (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

- mit internationalem Recherchenbericht (Artikel 21 Absatz 3)
- vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eingehen (Regel 48 Absatz 2 Buchstabe h)

connected to the spatial zone controller (14, 18) and provides an access control list (ACL), wherein the access control list determines a network access restriction depending on device information and spatial positions. The spatial zone controller (14, 18) is designed to compare the received device information and the determined spatial position with the access control list (ACL) in order to ascertain a corresponding network access restriction for the logging-in terminal (32) and/or the external wireless access point, and, depending on the result, to prevent the logging-in terminal and/or the external wireless access point from accessing the network.

(57) **Zusammenfassung:** Ein System (20) zum Bereitstellen eines drahtlosen Netzwerks umfasst eine Vielzahl von drahtlosen Zugangspunkten (10, 10'), die jeweils einen begrenzten Raumbereich in einem Gebäude (1, 1') oder einer baulichen Anlage mit einem Zugang zu dem drahtlosen Netzwerk versorgen. Ferner ist wenigstens ein Raumzonencontroller (14, 18) vorgesehen, der mit zumindest einem Teil der drahtlosen Zugangspunkten verbunden und ausgelegt ist, eine Geräteinformation eines sich im Netzwerk anmeldenden Endgeräts (32) und/oder externen drahtlosen Zugangspunkts über die mit ihm verbundenen drahtlosen Zugangspunkte zu empfangen und anhand einer Zuordnung zu einem oder mehreren der verbundenen drahtlosen Zugangspunkte die räumliche Position des betreffenden Endgeräts (32) und/oder externen drahtlosen Zugangspunkts in oder nahe dem Gebäude (1) oder der baulichen Anlage zu bestimmen. Außerdem ist ein zentraler Sicherheitscontroller (24) vorgesehen, der mit dem Raumzonencontroller (14, 18) verbunden ist und eine Zugangskontrollliste (ACL) bereitstellt, wobei die Zugangskontrollliste eine Netzzugangsbeschränkung abhängig von Geräteinformationen und räumlichen Positionen festlegt. Der Raumzonencontroller (14, 18) ist ausgelegt, die empfangene Geräteinformation und die bestimmte räumliche Position mit der Zugangskontrollliste (ACL) zu vergleichen, um eine entsprechende Netzzugangsbeschränkung für das sich anmeldende Endgerät (32) und/oder den externen drahtlosen Zugangspunkt zu ermitteln, und abhängig von dem Ergebnis das sich anmeldende Endgerät und/oder den externen drahtlosen Zugangspunkt am Netzzugang zu hindern.

SYSTEM ZUM BEREITSTELLEN EINES DRAHTLOSEN NETZWERKS

BESCHREIBUNG

5 Technisches Gebiet

Die vorliegende Erfindung betrifft ein System zum Bereitstellen eines drahtlosen Netzwerks, das eine Vielzahl von drahtlosen Zugangspunkten umfasst, die jeweils einen begrenzten Raumbereich in einem Gebäude oder einer baulichen Anlage mit
10 einem Zugang zu dem drahtlosen Netzwerk versorgen können.

Stand der Technik

Solche raum- oder etagenübergreifende drahtlosen Netzwerke (WLAN, wireless local
15 area network) gehen üblicherweise über den Umfang gewöhnlicher Heimnetzwerke hinaus. Werden solche drahtlosen Netzwerke entsprechend im sogenannten Infrastrukturmodus betrieben, dann stellen in der Regel zentrale Router eine Anbindung an weitere Netzwerke, Netzwerksegmente oder das Internet her, wobei die drahtlo-
sen Zugangspunkte (engl. : wireless access points (AP), dt. auch Basisstation ge-
20 nannt) des Netzwerks mit dem Router kabelgebunden, z.B. über Ethernet, oder selbst auch drahtlos verbunden sein können. Im letzteren Fall fungieren die drahtlo-
sen Zugangspunkte allerdings eher als Wireless Bridges (point-to-point) oder Wirel-
ess Repeater (point-to-multipoint), denn als eigentliche Basisstation. In kleinen
Heimnetzwerken kann der Router selbst den drahtlosen Zugangspunkt beinhalten.

25

Die drahtlosen Zugangspunkte versorgen jeweils einen ihrer Reichweite entspre-
chenden Raumbereich mit einer Radiofrequenzstrahlung in den Frequenzintervallen
von z.B. 2.400 bis 2.483,5 GHz, von 5.150 bis 5.350 bzw. 5.470 bis 5.725 GHz, oder
weiteren Intervallen zwischen 1 und 7 GHz oder um 60 GHz, die aktuell noch in der
30 Diskussion sind. Sie senden mit dieser RF-Strahlung in kurzen zeitlichen Intervallen
sogenannte Beacons ("Leuchtfeuer" oder "-baken") aus, die Informationen bezüglich
des Netzwerknamens (SSID: service set identifier, bzw. im Infrastrukturnetzwerk die

sogenannte ESSID: extended service set identifier), der unterstützten Übertragungsraten sowie des Typs der Verschlüsselung der zu übertragenden Daten beinhalten.

- 5 Um ein Gebäude mit z.B. mehreren Räumen und/oder Etagen oder auch eine bauliche Anlage wie etwa einen Firmen- oder Universitäts- oder Forschungscampus oder eine Messe mit mehreren Gebäuden/Hallen und/oder einen Außenbereich mit Pavil-
- 10 lons oder ähnlichem wie bei einem Flughafen oder Bahnhof mit einem den entsprechenden Raumbereich abdeckenden Drahtlos-Netzwerk zu versorgen kann dieses in einem Extended Service Set Modus betrieben werden, bei dem – wie eingangs be-
- schrieben – die einzelnen drahtlosen Zugangspunkte z.B. über ein Ethernet miteinander verbunden sind und ein gemeinsames Funknetzwerk mit gemeinsamen
- Netzwerknamen (ESSID) aufspannen. Dadurch können Netzwerke mit großer Reichweite und befriedigender räumlicher Abdeckung erhalten werden.
- 15 Endgeräte (clients) mit z.B. intern vorgesehenem oder extern angeschlossenem, drahtlosen Adapter (wireless adapter) können sich im Funknetzwerk an- und abmelden, soweit sie sich in dem entsprechenden Raumbereich eines der drahtlosen Zu-
- gangspunkte befinden, und – soweit es sich um mobile Endgeräte handelt – sie können zwischen verschiedenen drahtlosen Zugangspunkten übergeben werden (Ro-
- 20 aming), wenn sie den Raumbereich des einen Zugangspunkts verlassen und denjenigen eines anderen Zugangspunkts erreichen, oder von diesem einfach ein stärkeres Signal erhalten. Die entsprechende Funktionalität kann im Endgerät und/oder auf Seiten der miteinander kommunizierenden Zugangspunkte realisiert sein.
- 25 Um eine optimale Abdeckung von Gebäuden oder baulichen Anlagen zu erhalten und gleichzeitig Kosten und Aufwand für die Verkabelung und die Anzahl der Geräte zu sparen, werden herkömmlich darin an ausgewählten Standorten leistungsstarke drahtlose Zugangspunkte mit großer Reichweite platziert, die jeweils für sich Endge-
- 30 räte innerhalb eines großen Raumbereichs mit einem Funknetzwerk versorgen zu können. Dabei werden die zulässigen Maximalwerte von 100 mW isotrope Strahlungsleistung (EIRP) für das Intervall bei 2,4 GHz bzw. 200 mW, 500 mW oder 1.000 mW EIRP für die Intervalle bei 5 GHz (je nach Intervall und rechtlicher Lage im betreffenden Staat in Europa, Amerika oder Asien etc.) üblicherweise ausgeschöpft.

Gerade aufgrund der großen Leistungsstärke des ausgesandten Signals, die bei der herkömmlichen Grobmaschigkeit eines Funknetzwerks erforderlich ist, um auch abgelegene Nischen oder Raumbereiche mit abdecken zu können, dehnt sich oftmals der durch die Reichweite des jeweiligen Zugangspunkts überspannte Raumbereich deutlich über die Grenzen des Gebäudes oder der baulichen Anlage hinaus aus – z.B. in Räumen eines im gleichen Gebäude. Ein sich in diesem Außenbereich aufhaltendes Endgerät kann sich dabei z.B. durch sogenanntes "Sniffen" unerlaubt Zugang zum Funknetzwerk verschaffen, indem es über einen Zeitraum die Funkverbindung zwischen Zugangspunkt und (autorisiertem) Endgerät abhört und protokolliert, und dies auswertet um sich des oder der Netzwerkschlüssel zu bemächtigen (zum Beispiel sog. Known-Plaintext-Angriffe mit Sammeln von Schlüsselpaaren). Auch kann eine bloße Auswertung der nur vom drahtlosen Zugangspunkt wiederholt ausgesandten Beacons ausreichen, wenn der protokollierte Zeitraum hinreichend groß und die entsprechende Rechnerkapazität ist.

Darüber hinaus bzw. darauf aufbauend kann sich auch ein externer drahtloser Zugangspunkt Zugang zum Netzwerk verschaffen, indem er anhand entsprechender Informationen vorgibt, ein regulärer und autorisierter Zugangspunkt des Funknetzwerks zu sein, so dass sich Endgeräte im Netzwerk fälschlicherweise bei diesem anmelden und Daten übertragen, welches mit dem sogenannten "Snarfing" bezeichnet wird (z.B. sog. Janus- oder Man-in-the-middle-Angriffe).

Zwar stehen mit dem Nachfolger WPA2 (Wi-Fi protected access, konform mit IEEE 802,11i) des heutzutage als nicht mehr als zureichend geltenden, IEEE 802.11 konformen Verschlüsselungsstandards WEP (wired equivalent privacy) regelmäßig sichere Verschlüsselungstechniken zur Verfügung. Schwachstellen der Komponenten und Missbrauch sind jedoch nicht völlig auszuschließen.

Ein weiterer Baustein der Sicherheitsarchitektur ist ebenfalls regelmäßig eine Zugangskontrollliste, in der gerätespezifische Informationen aufgenommen sind, die z.B. eine Hardware-Kennung bzw. Adresse beinhalten. Nur den Endgeräten, die sich mit dieser in der Zugangskontrollliste hinterlegten Hardware-Adresse anmelden, wird

der Netzwerkzugang vom drahtlosen Zugangspunkt ermöglicht. Ein Beispiel ist die MAC-Adresse (media access control), die jedem einen Netzwerkadapter besitzen Gerät eindeutig zugeordnet ist (Microsoft: "physikalische Adresse", Apple: "Airport ID", "Ethernet-ID" oder "Wi-Fi-Adresse"). Durch entsprechende Maßnahmen könnten externe, nicht in der Zugangskontrollliste enthaltene Geräte-Adressen ausgeschlossen werden, das sogenannte MAC-Filtering.

Allerdings kann jede MAC-Adresse eines jeweiligen Netzwerkknotens leicht geänderte werden, da MAC-Adressen nicht vom Netzwerkadapter des betreffenden Endgeräts an den Zugangspunkt übertragen werden, welches als "Spoofing" bekannt ist. Vielmehr lesen dabei entweder das jeweilige Betriebssystem oder ein speziell eingerichteter Netzwerkmanager diese Adresse vom Adapter aus und übertragen diese an den Zugangspunkt. Die ausgelesene Adresse kann dabei durch eine geeignete Software verändert werden um ein anderes Endgerät vorzutäuschen. Anzumerken ist, dass bei der allgemeinen Kommunikation auf der Ebene des Data Link Layers (OSI-Schicht 2) zwischen Endgerät und drahtlosem Zugangspunkt solche Grundinformationen (Verschlüsselungstyp, Übertragungsgeschwindigkeit, MAC-Adresse etc.) regelmäßig unverschlüsselt übertragen werden, so dass das Spoofing nicht besonders erschwert ist. Die Verwendung von MAC-Filtern allein bietet infolgedessen nur einen eingeschränkten Schutz vor einem unerlaubtem Netzwerkzugang Dritter.

Darstellung der Erfindung

Es ist daher eine Aufgabe der Erfindung, ein System zum Bereitstellen eines drahtlosen Netzwerks vorzuschlagen, das die Sicherheit vor einem unerlaubtem Zugriff auf die in einem Netzwerk übertragenen Daten erhöht und die Stabilität eines solchen Funknetzwerks verbessert. Es ist auch eine Aufgabe, ein entsprechendes Verfahren bereitzustellen.

Die Aufgabe wird gelöst durch ein System zum Bereitstellen eines drahtlosen Netzwerks mit den Merkmalen von Patentanspruch 1 sowie durch ein entsprechendes Verfahren gemäß Patentanspruch 14. Vorteilhafte Weiterbildungen des erfindungsgemäßen Systems sind Gegenstand der abhängigen Ansprüche.

Die Lösung betrifft ein System zum Bereitstellen eines drahtlosen Netzwerks, das eine Vielzahl von drahtlosen Zugangspunkten umfasst, die jeweils einen begrenzten Raumbereich in einem Gebäude oder einer baulichen Anlage beziehungsweise die sich in diesem Raumbereich befindlichen Endgeräte (clients) mit einem Zugang zu dem drahtlosen Netzwerk versorgen. Das drahtlose Netzwerk kann ein Infrastruktur-
5 netzwerk mit einem kabelgebunden (Ethernet, KNX, DALI, etc.) mit den einzelnen drahtlosen Zugangspunkten verbundenen Router sein (z.B. auch ein Distribution System, DS), oder auch ein Ad-Hoc-Netzwerk und ohne weitere Verbindung zu anderen Netzwerken. Ferner ist das Netzwerk nicht auf bestimmte Technologien be-
10 schränkt, z.B. kann es ein mit der IEEE 802.11-Familie konformes Wi-Fi-Netzwerk sein, oder z.B. ein Zigbee-Netzwerk (IEEE 802.15.4).

Das Gebäude oder die bauliche Anlage selbst ist nicht Teil der beanspruchten Lösung, sondern bezeichnet vielmehr die Anwendung und den räumlichen Bezug des Drahtlosnetzwerks. Ein Gebäude umfasst z.B. mehrere Räume und/oder Etagen. Das Netzwerk kann auf Teile von Gebäuden beschränkt sein, die z.B. einem das Netzwerk betreibenden Unternehmen zugeordnet sind. Eine bauliche Anlage kann wie beschrieben etwa ein Firmen- oder Universitäts- oder Forschungscampus sein,
20 oder eine Messe mit mehreren Gebäuden/Hallen und/oder einen Außenbereich mit Pavillons oder ähnlichem, aber auch ein Flughafen oder Bahnhof. Kennzeichnend ist, dass Zonen mit erhöhten Anforderungen an die Netzwerksicherheit unmittelbar an öffentliche Zonen oder solche mit geringeren Anforderungen angrenzen können.

25 Ferner ist wenigstens ein Raumzonencontroller vorgesehen, der mit zumindest einem Teil der drahtlosen Zugangspunkten verbunden und ausgelegt ist, eine Geräteinformation eines sich im Netzwerk anmeldenden Endgeräts und/oder externen drahtlosen Zugangspunkts über die mit ihm verbundenen drahtlosen Zugangspunkte zu empfangen und anhand einer Zuordnung zu einem oder mehreren der verbunde-
30 nen drahtlosen Zugangspunkte die räumliche Position des betreffenden Endgeräts und/oder externen drahtlosen Zugangspunkts in oder nahe dem Gebäude oder der baulichen Anlage zu bestimmen.

Der Ausdruck Raumzonencontroller wird als Bezeichner für eine mit den drahtlosen Zugangspunkten verbundene Steuervorrichtung verwendet und impliziert, dass dieser speziell für eine der Teilmenge der Zugangspunkte entsprechende Raumzone eingerichtet ist. Die Teilmenge der mit dem Raumzonencontroller verbundenen Zugangspunkte deckt daher mit ihrer Strahlung vorzugsweise eine zusammenhängenden dreidimensionalen Raum ab ("Raumzone"). Diese Raumzone kann sich auch über die physikalische Grenze des Gebäudes oder Gebäudeteils (Etagenboden, -decke, Außenwand, Fenster) etc. hinaus erstrecken und ist durch die Reichweite der (äußeren) drahtlosen Zugangspunkte bestimmt.

Der Raumzonencontroller ist ausgelegt, anhand einer Zuordnung zu einem oder mehreren der verbundenen drahtlosen Zugangspunkte die räumliche Position eines Endgeräts und/oder eines externen drahtlosen Zugangspunkts in oder nahe dem Gebäude oder der baulichen Anlage zu bestimmen. Die Positionsbestimmung kann auf verschiedene Weise erfolgen. Im einfachsten Fall wird die Hardware-Adresse desjenigen Zugangspunkts mit einer (z.B. in einem Speicher hinterlegten) Positionsreferenzliste verglichen, an dem sich das Endgerät etc. anmeldet. Aus dieser Positionsreferenzliste ist die Position auslesbar und wird dem Endgerät etc. zugeordnet. Desweiteren können mehrere der Zugangspunkte, die mit dem Raumzonencontroller verbunden sind, eine Signalstärke ermitteln, mit der sie das Endgerät empfangen, woraufhin der Raumzonencontroller anhand der Positionsreferenzliste für die drahtlosen Zugangspunkte eine genaue räumliche Position mittels entsprechender Software-Algorithmen berechnen kann. Ferner ist grundsätzlich auch eine Positionsbestimmung aufgrund einer Messung der Signallaufzeit vom Endgerät zu einzelnen der drahtlosen Zugangspunkte (Triangulation) bzw. eine Messung der zeitlichen Differenz des Signalempfangs bei diesen möglich.

Bei der Position kann es sich aber Aspekten der Erfindung zufolge auch nur um die bloße Angabe der Raumzone als Ganzes handeln, d.h., das Ereignis dass sich das Endgerät bei einem der mit dem Raumzonencontroller verbundenen drahtlosen Zugangspunkte angemeldet hat. Dieser Aspekt ist relevant, wenn mehrere Raumzonencontroller vorgesehen sind und dadurch eine Unterteilung des gesamten Raumbereichs in Raumzonen erfolgt, die Positionen entsprechen und Informationen dar-

über zulassen, ob sich das Endgerät in einer für diese erlaubten oder nicht erlaubten Zone befindet.

Der Raumzonencontroller ist mit den drahtlosen Zugangspunkten über eine Datenlei-
5 tung verbunden, z.B. Ethernet, DALI, KNX, etc., oder drahtlos wiederum über WLAN
oder Zigbee, etc. Der Raumzonencontroller kann als elektronischer Baustein in ei-
nem Router vorgesehen sein, oder dezentral, z.B. in Verbindung mit einem der Zu-
gangspunkte, oder einer Wireless Bridge oder einem Wireless Repeater. Er kann
auch auf reiner Software-Ebene abgebildet sein, und als Computerprogramm rech-
10 nergestützt in einem Prozessor z.B. eines zentralen oder dezentralen Servers aus-
führbar sein.

Desweiteren ist ein zentraler Sicherheitscontroller vorgesehen, der mit dem Raum-
zonencontroller verbunden ist und eine Zugangskontrollliste (access control list, ACL)
15 bereitstellt, wobei die Zugangskontrollliste eine Netzzugangsbeschränkung abhängig
von Geräteinformationen und räumlichen Positionen festlegt. Die Netzzugangsbe-
schränkung kann dabei eine einfache Zugangserlaubnis oder –ablehnung/-
zurückweisung beinhalten, oder aber ein abgestuftes System mit auch eingeschränk-
ten Zugang bieten, etwa durch Verschaffen eines Zugangs zu einem "Dummy"-
20 Funknetzwerk, das lediglich für das Endgerät nutzlose Informationen wie beispiels-
weise Werbung des das Funknetzwerk betreibenden Unternehmens überträgt.

Von Bedeutung ist die Zuordnung der Netzzugangsbeschränkung zu einer räumli-
chen Position in der Zugangskontrollliste. Dies erlaubt es, die Position eines sich
25 anmeldenden Endgeräts als zusätzliches Kriterium dafür herzunehmen, ob der ge-
wünschte Netzwerkzugang für das spezielle Endgerät – ausgewiesen durch die Ge-
räteinformation wie beispielsweise seine Hardware- oder MAC-Adresse – gerechtfertigt ist oder nicht.

30 Wie eingangs beschrieben ist es nämlich möglich, bei einem Endgerät die an den
drahtlosen Zugangspunkt übertragene Geräteadresse zu ändern und dabei z.B. die-
jenige Adresse eines nach Mitschnitt von Kommunikation als ohne Zugangsbe-
schränkung nachgewiesenen Endgeräts auszuwählen und zu übertragen. Befindet

sich das Endgerät mit der Geräteadresse nun an einer Position in einem unerlaubten Bereich, beispielsweise außerhalb einer Raumbereichs, für den das Endgerät zugelassen ist, insbesondere außerhalb des Gebäudeteils in den Räumen eines benachbarten Unternehmens, kann der Netzzugang trotz gefälschter Geräteadresse wirksam verhindert werden.

Anders herum kann durch MAC-Filtering ein sich (aufgrund der ermittelten Position) innerhalb des zu schützenden Raumbereichs bewegendes oder befindliches Endgerät mit nicht autorisierter Geräteadresse identifiziert und am Netzzugang gehindert werden.

Dazu ist der Raumzonencontroller ausgelegt, die empfangene Geräteinformation und die bestimmte räumliche Position mit der Zugangskontrollliste zu vergleichen, um eine entsprechende Netzwerkszugangsbeschränkung für das sich anmeldende Endgerät und/oder den externen drahtlosen Zugangspunkt zu ermitteln, und abhängig von dem Ergebnis das sich anmeldende Endgerät und/oder den externen drahtlosen Zugangspunkt am Netzwerkzugang zu hindern.

Der wenigstens eine Raumzonencontroller und der zentrale Sicherheitscontroller können über eine kabelgebundene oder drahtlose Kommunikation miteinander verbunden sein, z.B. Ethernet, DALI, KNX, etc., oder drahtlos wiederum über WLAN oder Zigbee, etc. Ebenso wie der Raumzonencontroller kann der zentrale Sicherheitscontroller als elektronischer Baustein in einem Router vorgesehen sein, oder dezentral, z.B. in Verbindung mit einem der Zugangspunkte, oder einer Wireless Bridge oder einem Wireless Repeater. Er kann auch wie jener auf reiner Software-Ebene abgebildet sein, und als Computerprogramm rechnergestützt in einem Prozessor z.B. eines zentralen oder dezentralen Servers ausführbar sein. Der zentrale Sicherheitscontroller und die Raumzonencontroller können auch im gleichen Gerät oder im gleichen elektronischen Bauteil angeordnet sein bzw. als Programm zur Ausführung gebracht werden.

Einer besonders vorteilhaften Weiterbildung zufolge sind die drahtlosen Zugangspunkte der Vielzahl jeweils einer Leuchte in dem Gebäude oder der baulichen Anlage

zugeordnet und besitzen jeweils mit dieser eine gemeinsame Leistungsversorgung. Dabei kann mit Vorteil auf das in der Regel engmaschige Netz von Leuchten zurückgegriffen werden, wie sie oftmals in Büroräumen oder Fertigungshallen etc. vorliegen. Überdies bieten moderne Beleuchtungsanlagen zentrale Steuerungen und dafür angepasste Bussysteme (wie DALI oder KNX, oder auch das drahtlose Zigbee) zur Steuerung der einzelnen Leuchten der Beleuchtungsanlage. Diese Bussysteme sind regelmäßig schmalbandig, da keine hohen Anforderungen an die Übertragungsrate bestehen, weil oft lediglich Werte für die Einstellparameter für die Leuchten übermittelt werden und/oder in zeitlichen Abständen Sensorwerte abgerufen werden.

10

Bei dieser Weiterbildung können die Raumzonencontroller und/oder auch der zentrale Sicherheitsserver über solche Bussysteme verbunden werden, d.h., der oder die die Raumzonencontroller mit den drahtlosen Zugangspunkte in den Leuchten und die Raumzonencontroller mit dem zentralen Sicherheitscontroller. Es hat sich herausgestellt, dass auch für diese Anforderung das entsprechende Bussystem der Beleuchtungsanlage völlig ausreichend ist (d.h., z.B. DALI, KNX oder Zigbee), da es nur gelegentliche Anfragen sich anmeldender Geräte und entsprechende Sicherheitsprüfungen beim Vergleich mit der Zugangskontrollliste gibt.

15

20 Die Leistungsversorgung kann dagegen über dieses Bussystem oder über Ethernet erfolgen (PoE, Power over Ethernet).

Einer weiteren Weiterbildung zufolge sind die Vielzahl der drahtlosen Zugangspunkte in einem zusammenhängenden, engmaschigen, gitterartigen Netz angeordnet, so dass im Fall eines sich im Netzwerk anmeldenden Endgeräts anhand einer sich zeitlich verändernden Zuordnung zu den drahtlosen Zugangspunkten des gitterartigen Netzes dessen Position und Bewegung im Gebäude oder der baulichen Anlage lückenlos verfolgbar ist. Ein solches engmaschiges und vor allem gitterartiges Netz bringt den Vorteil mit sich, dass die Auflösung der Positionsbestimmung deutlich erhöht wird. Ferner sind in einem Gitter (wie zum Beispiel insbesondere bei einer Großraumbeleuchtung) Positionsreferenzlisten der Zugangspunkte einfach zu erstellen, insbesondere die einzelnen Positionen der Zugangspunkte bei der Installation leicht zu erfassen.

25

30

Ein besonderer Vorteil entsteht dabei dadurch, dass die Strahlungsleistung des einzelnen drahtlosen Zugangspunkts deutlich reduziert werden kann, da im engmaschigen Gitter der benachbarte Zugangspunkt näher liegt. Ferner können, wenn die Erfindung wie oben beschrieben in Kombination mit Leuchten erfolgt, Charakteristiken der Leuchten wie beispielsweise Reflektoren eingesetzt werden, um eine Richtwirkung der WLAN-Strahlung zu erzielen, so dass die entsprechende Raumzone im engmaschigen Gitter auf den gewünschten Raumbereich begrenzt werden kann, d.h. Angriffe von außen vermieden werden. Die isotrope RF-Strahlungsleistung EIRP der beteiligten drahtlosen Zugangspunkte in der Vielzahl und insbesondere der Teilmenge für die Raumzone beträgt rein beispielhaft 50 mW oder bei 2,4 GHz und 100 mW oder weniger bei 5 GHz.

Einer weiteren Weiterbildung der Erfindung zufolge ist der Raumzonencontroller nur mit solchen drahtlosen Zugangspunkten verbunden, die in einer Raumzone an einem Außenrand des zusammenhängenden, engmaschigen, gitterartigen Netzes gelegen sind. Dadurch kann ein innerer Raumbereich von ungeschützten bzw. öffentlich zugänglichen Bereichen außerhalb des Gebäudes oder Gebäudeteils abgeschirmt werden. Angreifende Endgeräte oder externe Zugangspunkte melden sich primär an drahtlosen Zugangspunkten der geschützten Raumzone an, wobei die räumliche Position dieser Endgeräte etc. vom entsprechenden Raumzonencontroller ermittelt werden kann. Die äußere Raumzone erlaubt es nun spezifische Massnahmen in Bezug auf die Angreifer zu unternehmen, beispielsweise ein Dummy-Netzwerk aufzubauen, das für die Angreifer nutzlose Informationen zur Verfügung stellt, oder mit nachfolgend zu beschreibenden Mitteln den Zugang zum Netzwerk des inneren Raumbereichs erschwert oder unmöglich macht.

Einer weiteren Weiterbildung der Erfindung zufolge sind eine erste und wenigstens eine zweite Raumzone festgelegt, die verschiedenen Abschnitten des Gebäudes, Gebäudeteils oder der baulichen Anlage entsprechen und denen jeweils unterschiedliche, räumlich zusammenhängend angeordnete Teilmengen der drahtlosen Zugangspunkte in dem Gebäude oder der baulichen Anlage zugeordnet sind. Für jede Raumzone ist ein entsprechender Raumzonencontroller vorgesehen. Der zentrale

- Sicherheitscontroller ist dabei mit allen Raumzonencontrollern verbunden und stellt diesen die Zugangskontrollliste bereit. Durch eine Positionsermittlung in z.B. einer der für den Zutritt verbotenen Zone können Endgeräte (Clients) ausgeschlossen werden. Falls sich ein Benutzer von der öffentlichen Raumzone („free zone“) in eine für den Zutritt verbotene Zone bewegt, könnte z.B. folgendes geschehen:
- seine Endgeräteadresse (MAC-Adresse) wird von der Whitelist in die Blacklist verschoben;
 - seine Anmeldung im Netzwerk bzw. eine Sitzung (Session) kann vom drahtlosen Zugangspunkt (Access Point) getrennt werden.
- 5 Eine Deauthentication oder alternativ eine lokale Reduzierung der Leistung (siehe unten) ist hier allerdings eher bevorzugt. Somit wäre eine Wechselwirkung zwischen den Raumzonen, d.h. Kommunikation zwischen den jeweiligen Raumzonencontrollern (abgesehen von der Anwendung einer zentralen Whitelist/Blacklist) grundsätzlich anwendbar (d.h. ein festgestelltes Ereignis in der einen Raumzone und getroffene
- 10 Abwehrmaßnahmen in der anderen). Dadurch wird es möglich verschiedene räumliche Sicherheitsstufen zu realisieren, z.B. öffentlich, nur firmenintern und beschränkt auf Spezialaufgaben (Entwicklung, Buchhaltung, Personal, Unternehmensleitung, Rechtsabteilung).
- 15
- 20 Einer weiteren Weiterbildung der Erfindung zufolge sind der oder die Raumzonencontroller ausgelegt, den Netzwerkzugang zu verhindern, indem er wenigstens einen der ihm zugeordneten drahtlosen Zugangspunkte veranlasst, wiederholt Deauthifizierungs-Frames mit einer aus der empfangenen Geräteinformation bestimmten spezifischen Hardware-Adresse des Endgeräts und/oder externen drahtlosen Zugangspunkts auszusenden. Durch diese auch Jamming genannte Verfahren wird das angreifende Endgerät bzw. der externe Zugangspunkt besonders wirksam und dauerhaft am Netzzugang gehindert. Allerdings ist dieser Aspekt voraussichtlich nicht kompatibel mit solchen Drahtlosnetzwerken, die konform mit IEEE 802.11w sind.
- 25
- 30 Einer weiteren Weiterbildung der Erfindung zufolge sind der oder die Raumzonencontroller ausgelegt, den Netzzugang zu verhindern, indem aus der empfangenen Geräteinformation eine spezifische Hardware-Adresse des Endgeräts ermittelt und mit einer Liste von Hardware-Adressen vergleicht, die in der Zugangskontrollliste

entweder als freigegeben oder alternativ als gesperrt vorgegeben sind. Wie beschrieben ist das MAC-Filtern in Kombination mit der Positionsbestimmung ein wirksames Mittel um Angreifer zu erfassen.

- 5 Einer weiteren Weiterbildung der Erfindung zufolge sind der oder die Raumzonencontroller ausgelegt, die verbundenen drahtlosen Zugangspunkte in einen Monitormodus zu schalten, um diese als WLAN-Sniffer zu betreiben, um die externen drahtlosen Zugangspunkte aufzuspüren und deren räumliche Position zu bestimmen. Als WLAN-Sniffer übertragen die Netzzugangspunkte dieser Raumzone keine Daten.
- 10 Diese Weiterbildung ist daher besonders vorteilhaft in Kombination mit einer im Randbereich des Netzwerks angeordneten Teilmenge bzw. Raumzone, die den inneren Raumbereich vom einem Bereich außerhalb des Gebäudeteils oder Gebäudes etc. abschirmt.
- 15 Einer weiteren Weiterbildung der Erfindung zufolge umfasst das System eine Benachrichtigungsvorrichtung, die mit dem Sicherheitscontroller und/oder dem Raumzonencontroller verbunden ist und im Fall eines aus dem Vergleich resultierenden nicht autorisierten Netzzugangs durch das Endgerät und/oder den externen Zugangspunkt eine Warnmeldung ausgibt, die den Zeitpunkt des nicht autorisierten
- 20 Netzzugangs, die Hardware-Adresse und die Position des Endgeräts und/oder des externen Zugangspunkts beinhaltet. Dadurch wird es möglich weitere gezielte Maßnahmen einzuleiten oder ein Angreiferprofil zu erstellen.

- Einer weiteren Weiterbildung der Erfindung zufolge ist der Raumzonencontroller ausgelegt, eine Leistung, mit welcher die drahtlosen Zugangspunkte Datenpakete übermitteln, für jeden drahtlosen Zugangspunkt individuell einzustellen, wobei, wenn der Raumzonencontroller infolge des Vergleichs mit der Zugangskontrollliste feststellt, dass das sich anmeldende Endgerät oder der externe drahtlose Zugangspunkt am Netzzugang zu hindern ist, der Raumzonencontroller die Leistung zumindest desjenigen drahtlosen Zugangspunkts, welcher der erfassten Position des Endgeräts oder
- 30 des externen drahtlosen Zugangspunkts entspricht, reduziert oder ganz abschaltet. Dadurch wird dem angreifenden Endgerät etc. die Möglichkeit genommen, Daten aus dem Netzwerk zu erhalten, und zwar genau dort, wo es sich aufhält. Die Sniffing-

- Funktion kann weiter aufrechterhalten werden, um eine Position zu ermitteln bzw. ein Bewegungsprofil zu erstellen. Die Leistungsreduktion oder –abschaltung bewegt sich mit dem angreifenden Endgerät weiter und bleibt dadurch mit Vorteil lokal begrenzt – der Angreifer sieht kein Netzwerk mehr. In Analogie zur dynamischen Anpassung von Leistung, mit der einzelne Leuchten einer Beleuchtungsanlage gezielt versorgt werden, um eine sich durch einen ansonsten dunklen Raum bewegend Person mit ausreichendem Licht zu versorgen, kann dieser Aspekt ebenfalls als "Swarming" bezeichnet werden.
- 5
- 10 Einer weiteren Weiterbildung dieses Aspekts zufolge ist der Raumzonencontroller ausgelegt, zusätzlich die Leistung derjenigen drahtlosen Zugangspunkte individuell zu reduzieren, die im Netz räumlich benachbart sind zu dem drahtlosen Zugangspunkt, welcher der erfassten Position des Endgeräts oder des externen drahtlosen Zugangspunkts entspricht. Mit dieser Erweiterung wird die Leistungsreduktion noch
- 15 besser lokal angepasst, um einerseits den Angreifer wirksam am Netzzugang zu hindern, andererseits aber auch die Auswirkungen auf andere Endgeräte, die sich in der Nähe befinden, so gering wie möglich zu halten.
- Einer entsprechenden Weiterbildung dieses Aspekts zufolge werden die Teilmenge
- 20 der drahtlosen Zugangspunkte auch im Fall einer Leistungsreduktion oder –abschaltung vom Raumzonencontroller wenigstens im Monitormodus weiterbetrieben. Der Raumzonencontroller verfolgt das im Netzwerk das angemeldete oder sich anmeldende Endgerät und/oder den externe drahtlose Zugangspunkt anhand einer sich zeitlich verändernden Zuordnung zu den drahtlosen Zugangspunkten des Net-
- 25 zes im Hinblick auf dessen Position und Bewegung durch die erste Raumzone verfolgt, und aktualisiert die Auswahl des- oder derjenigen drahtlosen Zugangspunkte, deren Leistung für die Datenübermittlung reduziert wird, anhand der verfolgten Position.
- 30 Einer weiteren Weiterbildung der Erfindung zufolge ist der Raumzonencontroller ausgelegt, eine Leistung, mit welcher die drahtlosen Zugangspunkte der ihm zugeordneten Teilmenge die Datenpakete übermitteln, für jeden drahtlosen Zugangspunkt individuell einzustellen, wobei der Raumzonencontroller die drahtlosen Zugangspunkte

im Regelbetrieb bei reduzierter oder abgeschalteter Leistung für die Übermittlung von Datenpaketen betreibt. Wenn der Raumzonencontroller die räumliche Position eines Endgeräts und/oder eines externen drahtlosen Zugangspunkts ermittelt und der Vergleich der Geräteinformation mit der Zugangskontrollliste ergibt, dass das sich anmeldende Endgerät nicht am Netzzugang zu hindern ist, erhöht der Raumzonencontroller die Leistung zumindest desjenigen drahtlosen Zugangspunkts und vorzugsweise auch von dessen räumlich benachbarten drahtlosen Zugangspunkten, welcher der räumlichen Position des Endgeräts und/oder eines externen drahtlosen Zugangspunkts entspricht.

Dieser Aspekt entspricht einer Umkehrung des vorigen Erfindungsaspekts des "Swarmings": hier wird das gesamte Netz bei reduzierter Strahlungsleistung betrieben und nur ausgewählte drahtlose Zugangspunkte werden hinsichtlich ihrer Leistung erhöht, in deren Bereich sich autorisierte Endgeräte befinden. Abgesehen von der Energieeinsparung und verringerter Strahlungsbelastung wird dadurch die Netzsicherheit erhöht, dass der Netzzugang für Angreifer an sich im Ganzen durch das für sie immer nur schwach oder gar nicht sichtbare Netzwerk erschwert ist.

Erfindungsgemäß ist auch ein Verfahren zum Bereitstellen eines drahtlosen Netzwerks vorgesehen. Es umfasst die Schritte:

Bereitstellen einer Vielzahl von drahtlosen Zugangspunkten, die jeweils einen begrenzten Raumbereich in einem Gebäude oder einer baulichen Anlage mit einem Zugang zu dem drahtlosen Netzwerk versorgen,

Bereitstellen eines Raumzonencontrollers, der mit zumindest einem Teil der drahtlosen Zugangspunkten verbunden und ausgelegt ist, eine Geräteinformation eines sich im Netzwerk anmeldenden Endgeräts und/oder externen drahtlosen Zugangspunkts über die mit ihm verbundenen drahtlosen Zugangspunkte zu empfangen und anhand einer Zuordnung zu einem oder mehreren der verbundenen drahtlosen Zugangspunkte die räumliche Position des betreffenden Endgeräts und/oder externen drahtlosen Zugangspunkts in oder nahe dem Gebäude oder der baulichen Anlage zu bestimmen, und

Bereitstellen eines zentralen Sicherheitscontrollers, der mit dem Raumzonencontroller verbunden ist und eine Zugangskontrollliste bereitstellt, wobei die Zu-

gangskontrollliste eine Netzzugangsbeschränkung abhängig von Geräteinformationen und räumlichen Positionen festlegt,

wobei der Raumzonencontroller ausgelegt ist, die empfangene Geräteinformation und die bestimmte räumliche Position mit der Zugangskontrollliste zu vergleichen, um eine entsprechende Netzwerkszugangsbeschränkung für das sich anmeldende Endgerät und/oder den externen drahtlosen Zugangspunkt zu ermitteln, und abhängig von dem Ergebnis das sich anmeldende Endgerät und/oder den externen drahtlosen Zugangspunkt am Netzwerkzugang zu hindern.

- 10 Es ergeben sich dieselben Vorteile, wie sie mit Bezug auf das System und deren Weiterbildungen beschrieben wurden.

Weitere Vorteile, Merkmale und Einzelheiten der Erfindung ergeben sich aus den Ansprüchen, der nachfolgenden Beschreibung bevorzugter Ausführungsformen sowie anhand der Zeichnungen. In den Figuren bezeichnen gleiche Bezugszeichen gleiche Merkmale und Funktionen.

Kurze Beschreibung der Zeichnung(en)

- 20 Es zeigen:

Fig. 1 in schematischer Darstellung eine Draufsicht auf einen Grundriss einer Etage eines Gebäudes mit einer Anordnung von Leuchten und einem drahtlosen Zugangspunkten im Zentrum der Anordnung in einem System gemäß dem Stand der Technik;

Fig. 2 in schematischer Darstellung eine Draufsicht auf einen Grundriss einer Etage eines Gebäudes mit einer Anordnung von Leuchten und diesen jeweils zugeordneten drahtlosen Zugangspunkten in Raumzonen eines Systems zum Aufbauen eines drahtlosen Netzwerks gemäß einem ersten Ausführungsbeispiel der Erfindung;

Fig. 3 wie Fig. 2, jedoch gemäß einer Abwandlung des Ausführungsbeispiels;

Fig. 4 ein Blockdiagramm mit einer Übersicht über das System gemäß dem ersten Ausführungsbeispiel;

5 Fig. 5 ein Flussdiagramm zur Erläuterung der Funktionsweise des Systems aus Fig. 4;

Fig. 6. ein schematisches Diagramm zur Erläuterung des im ersten und zweiten Ausführungsbeispiel eingesetzten Jammings;

10

Fig. 7 in schematischer Darstellung eine Draufsicht auf einen Grundriss einer Etage eines Gebäudes mit einer Anordnung von Leuchten und diesen jeweils zugeordneten drahtlosen Zugangspunkten in Raumzonen eines Systems zum Aufbauen eines drahtlosen Netzwerks gemäß einem zweiten Ausführungsbeispiel der Erfindung;

15

Bevorzugte Ausführungsform(en) der Erfindung

Als Vergleichsbeispiel zur Erfindung ist in Fig. 1 ein herkömmliches System zum Aufbau eines Funknetzwerks skizziert. In der schematischen Darstellung ist in Draufsicht der Grundriß einer Etage eines Gebäudes bzw. Gebäudeteils 1 zu sehen, der von Außenwänden 2 begrenzt ist. Im Innern 6 des Gebäudes ist eine Deckenbeleuchtung vorgesehen, die aus einer Matrix bzw. aus einem Gitter von Leuchten 4 besteht, die folglich z.B. in Reihen und Spalten mit jeweils geeigneten Abständen untereinander angeordnet sind, um eine möglichst homogene Ausleuchtung des gezeigten Raums 2a in der Etage des Gebäudes bzw. Gebäudeteils 1 zu erzielen. Jede Leuchte 4 kann unmittelbar einem oder mehreren darunter befindlichen Arbeitsplätzen (nicht gezeigt) zugeordnet sein. Es kann sich z.B. um ein Großraumbüro handeln.

25

30 Ein Drahtlos- bzw. Funknetzwerk kann in dem Gebäude oder Gebäudeteil 1 durch jeweils einen drahtlosen Zugangspunkt 9 (wireless access point (AP)) je Etage aufgebaut werden. Es ist auch möglich, dass lediglich ein Zugangspunkt 9 überhaupt vorgesehen ist. Der Zugangspunkt 9 kann mit einem Router verbunden sein, so dass

vermittels einer Bridge und einem Switch (nicht gezeigt) ein Zugang zu einem Netzwerk im Internet hergestellt werden kann. Switch, Bridge, Router und Zugangspunkt 9 können in ein und demselben Gerät eingerichtet sein.

- 5 Die Leistung der im Raum 2a abgestrahlten Strahlung ist so ausgelegt, dass auch solche Endgeräte (clients), die sich beispielsweise in den Ecken des Raums 2a, z.B. unter der Leuchte 4 oben links in Fig. 1, befinden, eine ausreichende Strahlungsin-
- 10 tensität erhalten, um eine stabile Verbindung mit dem drahtlosen Zugangspunkt 9 aufbauen zu können. Strahlt der drahtlose Zugangspunkt 9 z.B. wie die Leuchten 4 von der Decke aus weitgehend isotrop zumindest in die Ebene der Etage hinein, so folgt daraus, dass – wie in Fig.1 durch die strichpunktierte Linie angedeutet ist, die ein Reichweite 9a des drahtlosen Zugangspunkts 9 wiedergibt – auch in einem Be-
- 15 reich 8 außerhalb des Gebäudes bzw. Gebäudeteils 1, nämlich in dem durch Schraffur gekennzeichneten Bereich 8a, eine Versorgung etwaiger dort befindlicher Endgeräte mit einem Netzwerkzugang möglich ist, vorausgesetzt, dass die Außenwände im Wesentlichen durchlässig für die Radiofrequenzstrahlung sind. Durch den hier nur einen drahtlosen Zugangspunkt 9 (z.B. je Etage, Raum oder Großraumbüro) sowie die Geometrie des Grundrisses ist dieser Bereich 8a hier besonders groß.
- 20 Ein erstes Ausführungsbeispiel eines Systems zum Aufbau eines drahtlosen Netzwerks, hier ein IEEE 802.11 konformes WLAN- oder Wi-Fi-Netzwerk, das diesen Nachteil beheben kann, ist in Fig. 2 dargestellt. Die Gegebenheiten des Gebäudes bzw. Gebäudeteils 1 mit Außenwänden 2 und Raum 2a darin seien identisch zum Vergleichsbeispiel der Fig. 1. Hier ist jeder Leuchte 4 im Raum 2a jeweils ein drahtlo-
- 25 ser Zugangspunkt 10 bzw. 10' zugeordnet. Die Leuchten werden z.B. durch ein aus der Gebäudeautomation bekanntes Kommunikationssystem von einer Steuervorrichtung zentral gesteuert. Jeder drahtlose Zugangspunkt 10, 10' kann integral mit der Leuchte (z.B. in der Raumdecke) verbaut sein, indem er z.B. auf deren Rahmen oder Reflektor für seine Antennenfunktion und/oder auf einen gemeinsamen Controller
- 30 und/oder Verkabelungsanschluss/Datenanbindung (Ethernet, DALI, KNX etc.) zurückgreift. Ein Vorteil besteht darin, dass dort, wo Licht für Arbeitsplätze benötigt wird, dann regelmäßig auch Bedarf für einen Netzwerkanschluss besteht. Die Strahlungsleistung für die Vielzahl von drahtlosen Zugangspunkten 10, 10' kann in diesem

Ausführungsbeispiel deutlich niedriger ausgeführt werden, z.B. deutlich unter der maximal zulässigen Strahlungsleistung liegen, etwa bei 50 mW oder weniger für 2,4 GHz und/oder 100 mW oder weniger für 5 GHz-Frequenzintervalle. Beispielsweise können die Reichweiten von Licht und RF-Strahlung aneinander angepasst werden.

5

Durch die Zuordnung der drahtlosen Zugangspunkte 10, 10' zu den Leuchten 4 entsteht eine räumlich gitterartige und engmaschige Netzanordnung 12 mit hoher Positionsauflösung.

10 Wie schematisch in Fig. 2 zu sehen ist, ist der schraffierte Bereich 8b in einem Bereich 8 außerhalb des Innern 6 des Gebäudes bzw. Gebäudeteils 1, in welchem ein Netzwerkzugang noch möglich ist, deutlich verringert im Vergleich zur Situation in Fig. 1, so dass auch die Sicherheit des Funknetzwerks verbessert ist.

15 In diesem ersten Ausführungsbeispiel bilden die drahtlosen Zugangspunkte 10', die räumlich am Rande der Netzanordnung 12 gelegen sind, eine erste Raumzone 6a aus, während die nicht am Rande gelegenen eine zweite Raumzone 6b ausbilden. Die Raumzonen 6a, 6b bezeichnen denjenigen Raum, der von den jeweiligen drahtlosen Zugangspunkten 10, 10', die der betreffenden Raumzone 6a, 6b logisch zugeordnet sind, durch Strahlung und Empfang für den Netzwerkzugang abgedeckt wird.
20 Die Raumzonen 6a, 6b sind vorzugsweise jeweils für sich zusammenhängende Raumbereiche.

Die drahtlosen Zugangspunkte 10' der ersten Raumzone 6a sind mit einem ersten
25 Raumzonencontroller 14 (engl.: area controller) über eine Datenleitung 16 verbunden, wie aus Fig. 4 zu sehen ist, die den Aufbau des Systems 20 zeigt. Bei der Datenleitung 16 kann es sich kabelgebunden um Ethernet, oder einen DALI-Bus (DALI, gemäß Normenfamilie IEC 62386, DALI steht für „Digital adressierbare Schnittstelle für die Beleuchtung“), KNX-Bus, oder nicht kabelgebunden um ZigBee oder auch
30 WLAN selbst handeln etc.

Desgleichen sind die drahtlosen Zugangspunkte 10 der zweiten Raumzone 6b mit einem zweiten Raumzonencontroller 18 (area controller) über eine entsprechende Datenleitung 16 verbunden.

- 5 Der erste Raumzonencontroller 14 ist dabei ausgelegt, einzelne oder mehrere der mit ihm verbundenen drahtlosen Zugangspunkte 10' so zu steuern, dass eine oder mehrere der nachfolgend beschriebenen Abwehrmaßnahmen gegen potentielle Angreifer zur Geltung kommen, die insbesondere sich im Außenbereich 8 befindliche Endgeräte betreffen, wenn sich diese über einen der drahtlosen Zugangspunkte 10' einen
10 Zugang zum internen Netzwerk verschaffen wollen (beispielsweise durch Netzwerk-anmeldung).

Eine erste Maßnahme besteht darin, das betreffende Endgerät zu identifizieren und Im Fall mangelnder Autorisierung zurückzuweisen. Zunächst ist dazu eine spezifische Geräteinformation wie etwa die an und für sich eindeutige MAC-Adresse (Media-Access-Control-Adresse) als Hardwareadresse des betreffenden Endgeräts zu be-
15 stimmen und diese später mit einer Zugangskontrollliste zu vergleichen. Bei Ethernet umfasst die MAC-Adresse insgesamt 48 Bit bzw. 6 Bytes, die oftmals in hexadezimaler Schreibweise vorliegen und byteweise durch Doppelpunkte getrennt geschrieben
20 werden. Der erste Raumzonencontroller 14 empfängt diese Daten von dem entsprechenden drahtlosen Zugangspunkt 10' bei der Kontaktaufnahme/Anmeldung des Endgeräts über die Datenleitung 16.

Fig. 4 zeigt dazu ferner einen mit dem ersten Raumzonencontroller 14 sowie auch
25 den zweiten Raumzonencontroller 18 über eine Datenleitung 22 verbundenen Sicherheitscontroller 24 (security controller). Dieser hält die Zugangskontrollliste zentral vor. Die Zugangskontrollliste umfasst eine sogenannte "Whitelist" mit allen Endgeräten bzw. deren MAC-Adressen, denen Zugang zum Netzwerk zu gewähren ist, und/oder eine sogenannte "Blacklist" mit allen solchen Endgeräten bzw. deren MAC-
30 Adressen, denen ein Zugang zum Netzwerk ausdrücklich zu verweigern ist. Solche Zugangskontrolllisten können in einer Tabelle in einer Datei bzw. in einer Datenbank hinterlegt sein.

Wie in Fig. 4 dargestellt ist, ist der Sicherheitscontroller 24 ferner mit über eine Datenleitung 26 mit einer Administrationsschnittstelle 28 verbunden, beispielsweise ein Web-Interface oder eine Terminal oder Rechner mit secure-shell (SSH) Zugriff auf die entsprechende Konfigurationsdatei, um die Zugangskontrollliste zu konfigurieren und zu pflegen. Ferner ist der Sicherheitscontroller 24 auch mit einer externen Benachrichtigungsvorrichtung 30 verbunden, die Warnmeldungen bei festgestellten Angriffen nicht autorisierter Endgeräte etc. z.B. an den Nutzer, Anwender oder Netzbetreiber ausgibt.

- 10 Der erste Raumzonencontroller 14 führt den Vergleich der empfangenen MAC-Adresse mit der Liste gültiger MAC-Adressen (Whitelist) oder ungültiger MAC-Adressen (Blacklist) in der Zugangskontrollliste durch. Dies kann in Form einer Anfrage (request) an den Sicherheitscontroller 24 erfolgen, bei der der erste Raumzonencontroller 14 die MAC-Adresse sendet und er ein Feedback vom Sicherheitscontroller 24 bzw. der ihn bildenden bzw. von ihm verwalteten Datenbank oder Tabelle erhält, ob ein Treffer vorliegt oder nicht, oder indem er jeweils aktuell oder regelmäßig die komplette Zugangskontrollliste lädt und selbst einzeln vergleicht.

- 20 Stellt der erste Raumzonencontroller 14 fest, dass eine Verletzung vorliegt, hindert er den Zugang des betreffenden Endgeräts durch eine Zurückweisung.

- 25 Eine weitere oder alternative Maßnahme besteht darin, wenigstens einen der dem Raumzonencontroller 14 zugeordneten drahtlosen Zugangspunkte veranlassen, wiederholt Deauthentifizierungs-Frames mit der aus der empfangenen Geräteinformation bestimmten MAC-Adresse des Endgeräts auszusenden. Dies wird als Jamming bezeichnet. Das Endgerät wird dadurch wiederholt veranlasst, von sich aus automatisch den Netzwerkzugang zu beenden. Es kommt daher nie zu einem wirksamen dauerhaften Netzwerkzugang.

- 30 Die Situation ist in einem modifizierten Ausführungsbeispiel in Fig. 6 dargestellt. Hierbei sendet wie beschrieben einer der drahtlosen Zugangspunkte 10' der Raumzone 6a wiederholt Deauthentifizierungs-Frames an das Endgerät 32 (hier rein schematisch als Smartphone dargestellt). Diese sind aber dergestalt, dass sich das

Endgerät 32 von einem anderen drahtlosen Zugangspunkt 10, und zwar in der inneren Raumzone 6b abmeldet bzw. zu diesem seine Verbindung wiederholt beendet.

Da es wie eingangs beschrieben möglich ist, auf Seiten des Betriebssystems oder auf Softwareebene die vom Endgerät übermittelte MAC-Adresse zu ändern, insbesondere auf eine als vom Netzwerk als autorisierte betrachtete MAC-Adresse, welches für Dritte durch Sniffing festgestellt werden kann, werden in diesem Ausführungsbeispiel noch weitere Maßnahmen getroffen, um die Autorisation des Endgeräts zu prüfen.

Der Raumzonencontroller 14 ist dabei ausgelegt, dem sich anmeldenden Endgerät eine Position zuzuordnen bzw. diese zu bestimmen. Die Position kann die Raumzone 6a selbst sein, oder die Position desjenigen drahtlosen Zugangspunkts 10', bei dem sich das Endgerät anzumelden versucht. Ferner kann eine genaue Positionsbestimmung erfolgen, indem für mehrere drahtlose Zugangspunkte die Leistung des empfangenen Signals erfasst und miteinander in bezug auf die Position der drahtlosen Zugangspunkte 10' selbst verglichen wird. In Fig. 2 führt dies alles zu einer Lokalisierung in der Raumzone 6a nahe der Außenwand 2 und ggf. zu einer Unterscheidung, ob im Innern 6 des Raums 2a oder im Außenbereich 8. Diese Zusatzinformation erlaubt es dem ersten Raumzonencontroller 14, eine Bewertung anhand der Anmeldung des Endgeräts 32 durchzuführen. Dazu ist in der Zugangskontrollliste des weiteren eine Information dahingehend enthalten, ob das der MAC-Adresse zugeordnete Endgerät an dieser Position (d.h. in dieser Raumzone, oder bei diesem drahtlosen Zugangspunkt, oder an diesem genauen Standort) sich zu befinden autorisiert ist.

Der erste Raumzonencontroller 14 vergleicht dabei die vorzugsweise in der Zugangskontrollliste für diese MAC-Adresse hinterlegte Position (d.h. Raumzone, Bereich des drahtlosen Zugangspunkts, oder genauer Standort) mit der tatsächlich zugeordneten, und trifft daraus resultierend eine der genannten Maßnahmen.

Ist die MAC-Adresse weder in einer Whitelist noch in einer Blacklist, kann ein Default vorgesehen sein (z.B. Zugang für alle Adressen außer Blacklist, Zurückweisung etc für alle Adressen außer Whitelist, etc.).

Fig. 5 zeigt in einem Flussdiagramm einen Überblick über den Ablauf des Verfahrens: In einem Schritt 102 meldet sich ein (z.B. nicht autorisiertes) Endgerät 32 im Drahtlos-Netzwerk an, oder alternativ meldet sich im Schritt 104 ein externer drahtloser Zugangspunkt, der nicht Teil des Funknetzwerks ist, als Endgerät 32 an (z.B.

5 Man-in-the middle-Angriff).

Im Schritt 106 empfängt der drahtlose Zugangspunkt 10' die Geräteinformation und leitet diese an den ersten Raumzonencontroller 14 weiter.

10 Im Schritt 108 empfängt der erste Raumzonencontroller 14 die Geräteinformation und vergleicht diese mit einer verteilten Zugangskontrollliste (access controll list, ACL), die er ebenfalls übermittelt bekommen hat.

Dazu wird vorab in einem Schritt 110 die Zugangskontrollliste über ein Web-Interface
15 (Administrationsschnittstelle 28) konfiguriert und dabei eine Whitelist mit den für einen Netzwerkzugang autorisierten Endgeräten 32 erstellt, wobei die Whitelist bezogen auf Raumzonen ist, d.h., Netzwerkzugangsbeschränkungen in Bezug auf Positionen der Endgeräte enthält. In einem Schritt 112 wird diese Zugangskontrollliste in einer Tabelle oder Datenbank in dem zentralen Sicherheitscontroller 24 hinterlegt
20 und gespeichert. In einem Schritt 114 wird diese Zugangskontrollliste an die Raumzonencontroller 14, 18 verteilt (übermittelt), unter anderem an den ersten Raumzonencontroller 14.

In einem Schritt 116 berechnet der erste Raumzonencontroller 14 die Position des
25 Endgeräts 32 wie oben beschrieben, anhand der übermittelten Informationen von dem oder den verbundenen drahtlosen Zugangspunkten 10', und im Schritt 118 vergleicht der erste Raumzonencontroller 14 die ermittelte, bestimmte oder berechnete Position mit der in der Zugangskontrollliste hinterlegten (oder aus dieser ableitbaren) Position für Netzwerkzugang oder –zurückweisung für die MAC-Adresse. Im Fall,
30 dass der Vergleich zu einer Zurückweisung führt, wird der zentrale Sicherheitscontroller 24 im Schritt 120 veranlasst, eine Warnung in der Benachrichtigungsvorrichtung 30 auszugeben.

Ferner wird in diesem speziellen Ausführungsbeispiel im Schritt 122 der drahtlose Zugangspunkt 10' veranlasst, ein Deauthentikations-Frame auszusenden, so dass sich das Endgerät von einem z.B. anderen drahtlosen Zugangspunkt 10 abmeldet (d.h. Verbindung beendet).

5

Es ist anzumerken, dass die drahtlosen Zugangspunkte 10' des ersten Ausführungsbeispiels mit besonderem Vorteil auch im Monitormodus betrieben werden können, d.h., sie werden selbst gleichsam als Sniffer betrieben.

- 10 Mit Bezug auf Fig. 3 wird eine Abwandlung dieses ersten Ausführungsbeispiels beschrieben. Das gitterartige, engmaschige Netz 12 von drahtlosen Zugangspunkten wird dabei noch verfeinert, indem jeder Leuchte z.B. 4 vier drahtlose Zugangspunkte mit jeweils unterschiedlich ausgerichteten Antennen zugeordnet werden. Der ersten Raumzone 6a werden dabei nur die dem Außenbereich 8 am Rand des Netzes 12
- 15 zugewandten drahtlosen Zugangspunkte 40' zugeordnet, während die nach innen oder anderen, benachbarten Zugangspunkten zugewandten drahtlosen Zugangspunkte 40 sogar auch in Leuchten 4 nahe der Außenwand 2 der zweiten inneren Raumzone 6b zugeordnet sind. Dadurch wird die Raumzone 6a kleiner, so dass, wenn deren drahtlose Zugangspunkte 40' z.B. im Monitormodus betrieben werden,
- 20 mehr Raum für das eigentliche Netzwerk zur Verfügung steht.

- Mit Bezug auf Figur 7 wird ein zweites Ausführungsbeispiel beschrieben. In diesem Ausführungsbeispiel sind nicht mehr nur 2 Raumzonen, sondern vielmehr 3 Raumzonen festgelegt: eine öffentliche Raumzone 6c, eine Raumzone 6d mit eingeschränktem Netzwerkzugang sowie eine Raumzone 6e ohne Netzwerkzugang. Es
- 25 handelt sich z.B. um einen Kundenbereich, einen Flur oder Zwischentrakt und einen Sicherheitsraum im Gebäude 1 in dieser Reihenfolge. In Fig. 7 sind der Übersichtlichkeit halber nur noch die Leuchten 4, nicht mehr die drahtlosen Zugangspunkte gezeigt. Die Zuordnung von drahtlosen Zugangspunkte zu Leuchten ist aber hier wie
- 30 in Fig. 2 oder 3.

Das entsprechende System 1' ist konfiguriert wie in Fig. 4 und 5 gezeigt. In diesem Ausführungsbeispiel wird eine Zugangskontrollliste ACL konfiguriert, bei der ein

Raumzonencontroller (nicht gezeigt) für die Raumzone 6c z.B. weder eine Blacklist noch eine Whitelist führt. Eine Positionsinformation betrifft implizit die gesamte Raumzone für alle möglichen MAC-Adressen (die gesamte Raumzone alle Positionen in der Raumzone erlaubt).

5

Für die sicherheitsrelevanteren Raumzone 6d existiert z.B. eine Whitelist. Die entsprechende Positionsinformation betrifft implizit die gesamte Raumzone für alle MAC-Adressen der Whitelist. Für alle anderen möglichen MAC-Adressen ist die Position, d.h. die gesamte Raumzone mit allen enthaltenen drahtlosen Zugangspunkten ungültig und führt zu einer Warnmeldung.

10

In der absoluten Sicherheitszone, d.h. Raumzone 6e ist überhaupt kein Endgerät zugelassen. Die Positionsinformation betrifft implizit wieder die gesamte Raumzone 6e, nun für alle möglichen MAC-Adressen.

15

Bei dieser Ausführungsform gestufter Autorisierungen für Netzwerkzugänge können mit Vorteil auch Swarming-Verfahren wie oben beschrieben eingesetzt werden. Dabei wird eine Leistung, mit welcher die drahtlosen Zugangspunkte Datenpakete übermitteln, für jeden drahtlosen Zugangspunkt individuell eingestellt. Wenn der Raumzonencontroller infolge des Vergleichs mit der Zugangskontrollliste feststellt, dass das sich anmeldende Endgerät 32 am Netzwerkzugang zu hindern ist, mindert der entsprechende Raumzonencontroller lediglich lokal die Leistung des- oder derjenigen drahtlosen Zugangspunkte, welche der erfassten Position des Endgeräts oder des externen drahtlosen Zugangspunkts entsprechen. Mit Sniffing kann überdies eine Positionsermittlung aufrechterhalten um ein Bewegungsprofil zu erstellen. Die Leistungsreduktion oder –abschaltung bewegt sich mit dem nicht autorisierten Endgerät weiter und bleibt dadurch mit Vorteil lokal begrenzt – der Angreifer sieht kein Netzwerk mehr. In Analogie zur dynamischen Anpassung von Leistung, mit der einzelne Leuchten einer Beleuchtungsanlage gezielt versorgt werden, um eine sich durch einen ansonsten dunklen Raum bewegend Person mit ausreichendem Licht zu versorgen, kann dieser Aspekt ebenfalls als "Swarming" bezeichnet werden.

20

25

30

Es kann also auch die Bewegung eines Endgeräts durch das Netz von Zugangspunkten und ggf. durch die Raumzonen aufgezeichnet werden (Tracking). Abhängig vom Bewegungsprofil können sogar auch Maßnahmen getroffen werden. Bewegt sich ein Endgerät beispielsweise am Außenrand einer Raumzone von drahtlosem Zugangspunkt zu drahtlosem Zugangspunkt, so kann anhand des Profils eine Wahrscheinlichkeit angesetzt werden, dass sich das Endgerät möglicherweise an einer Wand außerhalb des eigentlichen Raumbereichs bewegt und daher nicht autorisiert ist. Hier können dann ebenfalls entsprechende Maßnahmen getroffen werden.

- 10 Es ist anzumerken, dass die oben beschriebenen Ausführungsbeispiele spezielle Ausführungsformen darstellen und den durch die beigefügten Ansprüche definierten Schutzzumfang nicht eingrenzen. Insbesondere können auch einzelne Merkmale der einzelnen Ausführungsbeispiele in jeweils andere Ausführungsbeispiele kombiniert werden. Beispielsweise, können Abwehrmaßnahmen wie MAC-Filtering, Jamming
15 (Aussenden von Deauthentikationssignalen), Swarming, auch kombiniert oder aber auch nur fallweise – je nach Schwerwiegen oder Art des Angriffs – vorgenommen werden.

In dieser Anmeldung kann der Ausdruck "Anmelden" durch das Endgerät als Registrierungsprozess mit einer Definition der Übertragungsparameter zwischen Endgerät und Zugangspunkt verstanden sein. Mit "anmelden" wird hier aber auch nur die bloße Aussendung von Datenpaketen durch das Endgerät verstanden, die in Antwort auf Beacons durch den Zugangspunkt erfolgen, d.h. das bloße in-Kontakt-treten. Ebenso schließt "Abmelden" ein bloßes Beenden der Verbindung ein.

25

In den Ausführungsbeispielen wurden die Raumzonencontroller 14, 18 und der Sicherheitscontroller 24 als über eine Datenleitung 22 verbunden beschrieben, welches eine physische Beschaffenheit als getrennte elektronische Bausteine implizieren könnte. Selbstverständlich können die Controller aber auch lediglich als getrennte
30 computerimplementierte Programme beschaffen sein, die auf getrennten wie aber auch demselben Rechner, Server oder lokalen Knoten laufen.

BEZUGSZEICHENLISTE:

1, 1'	Gebäude, Gebäudeteil, bauliche Anlage
2, 2a	Außenwand, Raum, Raumbereich
4	Leuchten
6	Inneres (Gebäude)
6a-e	Raumzonen
8	Außenbereich (Gebäude)
9	drahtloser Zugangspunkt (herkömmlich)
9a	Reichweite
10, 10'	drahtlose Zugangspunkte
10a	Reichweite
12	netzartige Anordnung von drahtlosen Zugangspunkten
14	Raumzonencontroller
16	Datenleitung
18	Raumzonencontroller
20	System zum Aufbauen eines drahtlosen Netzwerks
22	Datenleitung
24	Raumzonencontroller
26	Datenleitung
28	Administrationsschnittstelle
30	Benachrichtigungsvorrichtung
32	Endgerät
33	Aussenden von Deauthentikations-Frames
34	Beenden der Verbindung
40, 40'	drahtlose Zugangspunkte (gerichtete Antenne)
102	Anmelden eines Endgeräts

104	Anmelden eines externen drahtlosen Zugangspunkts
106	Empfang der MAC-Adresse und Weiterleiten (AP)
108	Empfang der MAC-Adresse durch Raumzonencontroller
110	Konfigurieren Zugangskontrollliste (ACL)
112	Speichern Zugangskontrollliste (ACL)
114	Verteilen ACL an Raumzonencontroller
116	Berechnen der Position
118	Vergleich von MAC-Adresse und Position mit ACL
120	Warnmeldung: Systemverletzung
ACL	Zugangskontrollliste

PATENTANSPRÜCHE:

1. System (20) zum Bereitstellen eines drahtlosen Netzwerks, umfassend:
eine Vielzahl von drahtlosen Zugangspunkten (10, 10'), die jeweils einen be-
5 grenzten Raumbereich in einem Gebäude (1, 1') oder einer baulichen Anlage mit ei-
nem Zugang zu dem drahtlosen Netzwerk versorgen,

wenigstens einen Raumzonencontroller (14, 18), der mit zumindest einem Teil
der drahtlosen Zugangspunkten verbunden und ausgelegt ist, eine Geräteinformation
eines sich im Netzwerk anmeldenden Endgeräts (32) und/oder externen drahtlosen
10 Zugangspunkts über die mit ihm verbundenen drahtlosen Zugangspunkte zu emp-
fangen und anhand einer Zuordnung zu einem oder mehreren der verbundenen
drahtlosen Zugangspunkte die räumliche Position des betreffenden Endgeräts (32)
und/oder externen drahtlosen Zugangspunkts in oder nahe dem Gebäude (1) oder
der baulichen Anlage zu bestimmen, und

15 einen zentralen Sicherheitscontroller (24), der mit dem Raumzonencontroller
(14, 18) verbunden ist und eine Zugangskontrollliste (ACL) bereitstellt, wobei die Zu-
gangskontrollliste eine Netzzugangsbeschränkung abhängig von Geräteinformatio-
nen und räumlichen Positionen festlegt,

wobei der Raumzonencontroller (14, 18) ausgelegt ist, die empfangene Gerä-
20 teinformation und die bestimmte räumliche Position mit der Zugangskontrollliste
(ACL) zu vergleichen, um eine entsprechende Netzzugangsbeschränkung für
das sich anmeldende Endgerät (32) und/oder den externen drahtlosen Zugangspunkt
zu ermitteln, und abhängig von dem Ergebnis das sich anmeldende Endgerät
und/oder den externen drahtlosen Zugangspunkt am Netzwerkzugang zu hindern.

25 2. System gemäß Anspruch 1, wobei
die drahtlosen Zugangspunkte der Vielzahl jeweils einer Leuchte in dem Ge-
bäude oder der baulichen Anlage zugeordnet sind und jeweils mit dieser eine ge-
meinsame Leistungsversorgung besitzen.

30 3. System gemäß Anspruch 1 oder 2, wobei
die Vielzahl der drahtlosen Zugangspunkte in einem zusammenhängenden,
engmaschigen, gitterartigen Netz angeordnet sind, so dass im Fall eines sich im

Netzwerk anmeldenden Endgeräts anhand einer sich zeitlich verändernden Zuordnung zu den drahtlosen Zugangspunkten des gitterartigen Netzes dessen Position und Bewegung im Gebäude oder der baulichen Anlage lückenlos verfolgbare ist.

5 4. System gemäß Anspruch 3, wobei
 der Raumzonencontroller nur mit solchen drahtlosen Zugangspunkten verbunden ist, die in einer Raumzone an einem Außenrand des zusammenhängenden, engmaschigen, gitterartigen Netzes gelegen sind.

10 5. System gemäß Anspruch 3 oder 4, wobei
 eine erste und wenigstens eine zweite Raumzone festgelegt sind, die verschiedenen Abschnitten des Gebäudes oder der baulichen Anlage entsprechen und denen jeweils eine unterschiedliche, räumlich zusammenhängend angeordnete Teilmengen der drahtlosen Zugangspunkte in dem Gebäude oder der baulichen Anlage
15 zugeordnet sind,
 wobei für jede Raumzone ein entsprechender Raumzonencontroller vorgesehen ist, und
 wobei der zentrale Sicherheitscontroller mit allen Raumzonencontrollern verbunden ist und diesen die Zugangskontrollliste bereitstellt.

20 6. System gemäß einem der Ansprüche 1 bis 5, wobei
 der oder die Raumzonencontroller ausgelegt sind, den Netzwerkzugang zu verhindern, indem er wenigstens einen der ihm zugeordneten drahtlosen Zugangspunkte veranlasst, wiederholt Deauthentifizierungs-Frames mit einer aus der emp-
25 fangenen Geräteinformation bestimmten spezifischen Hardware-Adresse des Endgeräts und/oder externen drahtlosen Zugangspunkts auszusenden.

 7. System gemäß einem der Ansprüche 1 bis 5, wobei
 der oder die Raumzonencontroller ausgelegt sind, den Netzzugang zu verhin-
30 dern, indem aus der empfangenen Geräteinformation eine spezifische Hardware-Adresse des Endgeräts ermittelt und mit einer Liste von Hardware-Adressen verglichen, die in der Zugangskontrollliste entweder als freigegeben oder alternativ als gesperrt vorgegeben sind.

8. System gemäß einem der Ansprüche 1 bis 7, wobei
der oder die Raumzonencontroller ausgelegt sind, die verbundenen drahtlosen
Zugangspunkte in einen Monitormodus zu schalten, um diese als WLAN-Sniffer zu
5 betreiben, um die externen drahtlosen Zugangspunkte aufzuspüren und deren räum-
liche Position zu bestimmen.

9. System gemäß einem der Ansprüche 1 bis 8, umfassend:
eine Benachrichtigungsvorrichtung, die mit dem Sicherheitscontroller und/oder
10 dem Raumzonencontroller verbunden ist und im Fall eines aus dem Vergleich resul-
tierenden nicht autorisierten Netzzugang durch das Endgerät und/oder den externen
Zugangspunkt eine Warnmeldung ausgibt, die den Zeitpunkt des nicht autorisierten
Netzzugangs, die Hardware-Adresse und die Position des Endgeräts und/oder des
externen Zugangspunkts beinhaltet.

15

10. System gemäß einem der Ansprüche 1 bis 9, wobei
der Raumzonencontroller ausgelegt ist, eine Leistung, mit welcher die drahtlo-
sen Zugangspunkte Datenpakete übermitteln, für jeden drahtlosen Zugangspunkt
individuell einzustellen,

20

wobei, wenn der Raumzonencontroller infolge des Vergleichs mit der Zu-
gangskontrollliste feststellt, dass das angemeldete oder sich anmeldende Endgerät
oder der externe drahtlose Zugangspunkt am Netzzugang zu hindern ist, der Raum-
zonencontroller die Leistung zumindest desjenigen drahtlosen Zugangspunkts, wel-
cher der erfassten Position des Endgeräts oder des externen drahtlosen Zugangs-
25 punkts entspricht, reduziert oder ganz abschaltet.

25

11. System gemäß Anspruch 10, wobei
der Raumzonencontroller ausgelegt ist, zusätzlich die Leistung derjenigen
drahtlosen Zugangspunkte individuell zu reduzieren, die im Netz räumlich benachbart
30 sind zu dem drahtlosen Zugangspunkt, welcher der erfassten Position des Endgeräts
oder des externen drahtlosen Zugangspunkts entspricht.

30

12. System gemäß Anspruch 10 oder 11, wobei

die Teilmenge der drahtlosen Zugangspunkte auch im Fall einer Leistungsreduktion oder –abschaltung vom Raumzonencontroller wenigstens im Monitormodus weiterbetrieben werden, und

5 der Raumzonencontroller im Netzwerk das angemeldete oder sich anmeldende Endgerät und/oder den externe drahtlose Zugangspunkt anhand einer sich zeitlich verändernden Zuordnung zu den drahtlosen Zugangspunkten des Netzes im Hinblick auf dessen Position und Bewegung durch die erste Raumzone verfolgt, und

10 die Auswahl des- oder derjenigen drahtlosen Zugangspunkte, deren Leistung für die Datenübermittlung reduziert wird, anhand der verfolgten Position aktualisiert wird.

13. System gemäß einem der vorhergehenden Ansprüche, wobei der Raumzonencontroller ausgelegt ist, eine Leistung, mit welcher die drahtlosen Zugangspunkte der ihm zugeordneten Teilmenge die Datenpakete übermitteln, für jeden drahtlosen Zugangspunkt individuell einzustellen,

wobei der Raumzonencontroller die drahtlosen Zugangspunkte im Regelbetrieb bei reduzierter oder abgeschalteter Leistung für die Übermittlung von Datenpaketen betreibt,

20 wobei, wenn der Raumzonencontroller die räumliche Position eines Endgeräts und/oder eines externen drahtlosen Zugangspunkts ermittelt und der Vergleich der Geräteinformation mit der Zugangskontrollliste ergibt, dass das angemeldete oder sich anmeldende Endgerät oder der externe Zugangspunkt nicht am Netzzugang zu hindern ist, der Raumzonencontroller die Leistung zumindest desjenigen drahtlosen Zugangspunkts und vorzugsweise auch von dessen räumlich benachbarten drahtlosen Zugangspunkten erhöht, welcher der räumlichen Position des Endgeräts

25 und/oder eines externen drahtlosen Zugangspunkts entspricht.

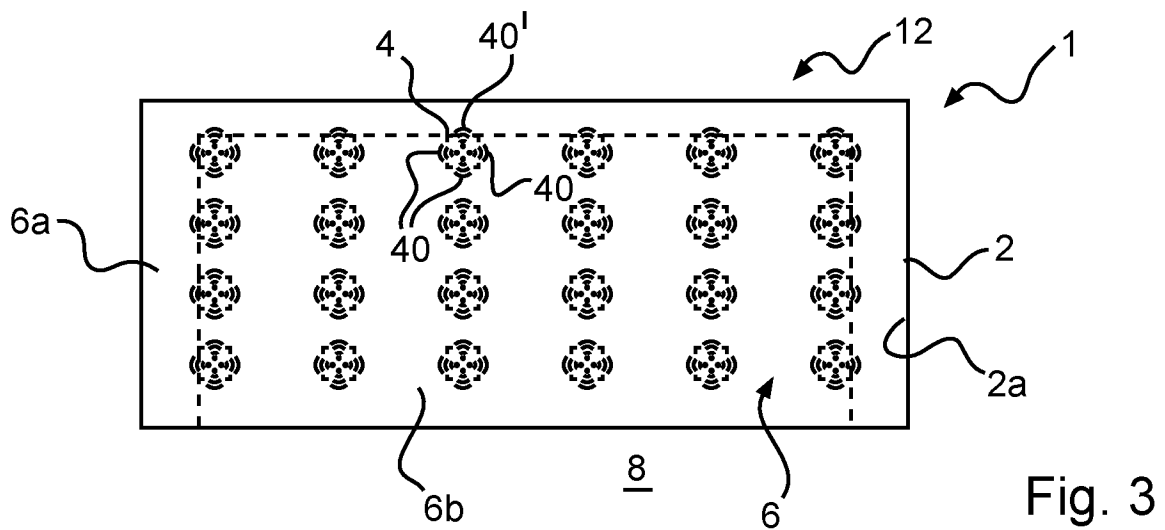
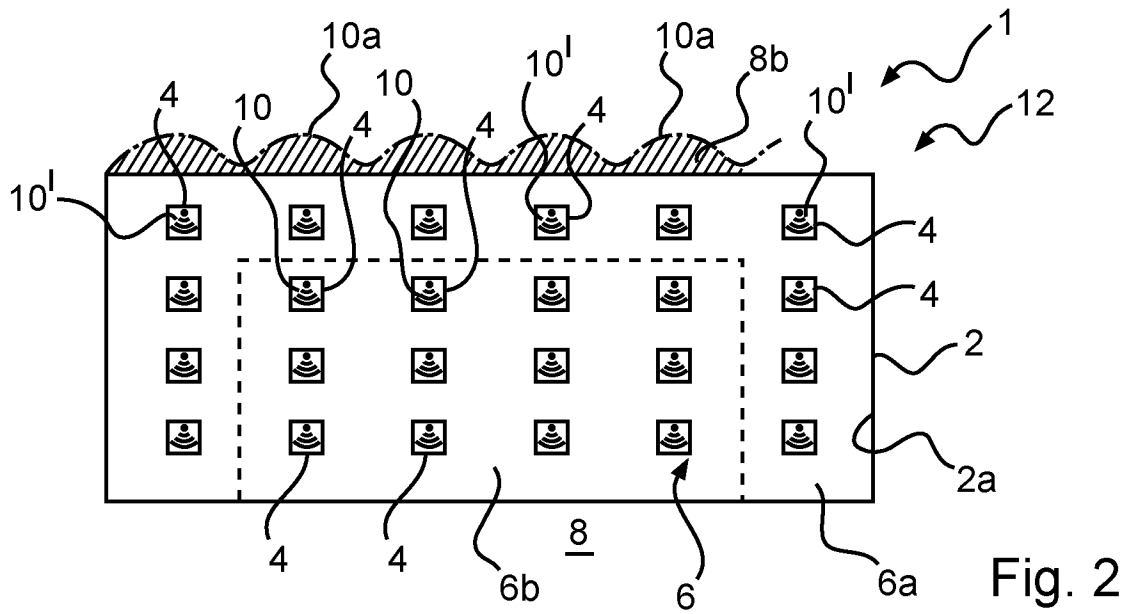
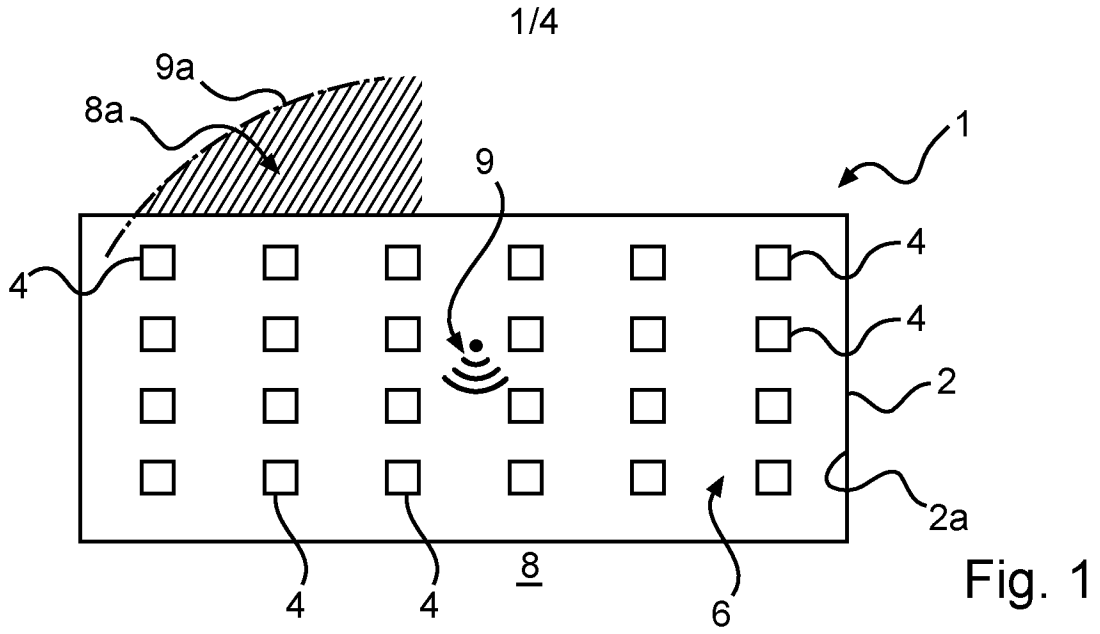
14. Verfahren zum Bereitstellen eines drahtlosen Netzwerks, umfassend: Bereitstellen einer Vielzahl von drahtlosen Zugangspunkten, die jeweils einen begrenzten Raumbereich in einem Gebäude oder einer baulichen Anlage mit einem Zugang zu dem drahtlosen Netzwerk versorgen,

Bereitstellen einen Raumzonencontroller, der mit zumindest einem Teil der drahtlosen Zugangspunkten verbunden und ausgelegt ist, eine Geräteinformation

eines sich im Netzwerk anmeldenden Endgeräts und/oder externen drahtlosen Zugangspunkts über die mit ihm verbundenen drahtlosen Zugangspunkte zu empfangen und anhand einer Zuordnung zu einem oder mehreren der verbundenen drahtlosen Zugangspunkte die räumliche Position des betreffenden Endgeräts und/oder externen drahtlosen Zugangspunkts in oder nahe dem Gebäude oder der baulichen Anlage zu bestimmen, und

Bereitstellen eines zentralen Sicherheitscontrollers, der mit dem Raumzonencontroller verbunden ist und eine Zugangskontrollliste bereitstellt, wobei die Zugangskontrollliste eine Netzzugangsbeschränkung abhängig von Geräteinformationen und räumlichen Positionen festlegt,

wobei der Raumzonencontroller ausgelegt ist, die empfangene Geräteinformation und die bestimmte räumliche Position mit der Zugangskontrollliste zu vergleichen, um eine entsprechende Netzwerkszugangsbeschränkung für das sich anmeldende Endgerät und/oder den externen drahtlosen Zugangspunkt zu ermitteln, und abhängig von dem Ergebnis das sich anmeldende Endgerät und/oder den externen drahtlosen Zugangspunkt am Netzwerkzugang zu hindern.



2/4

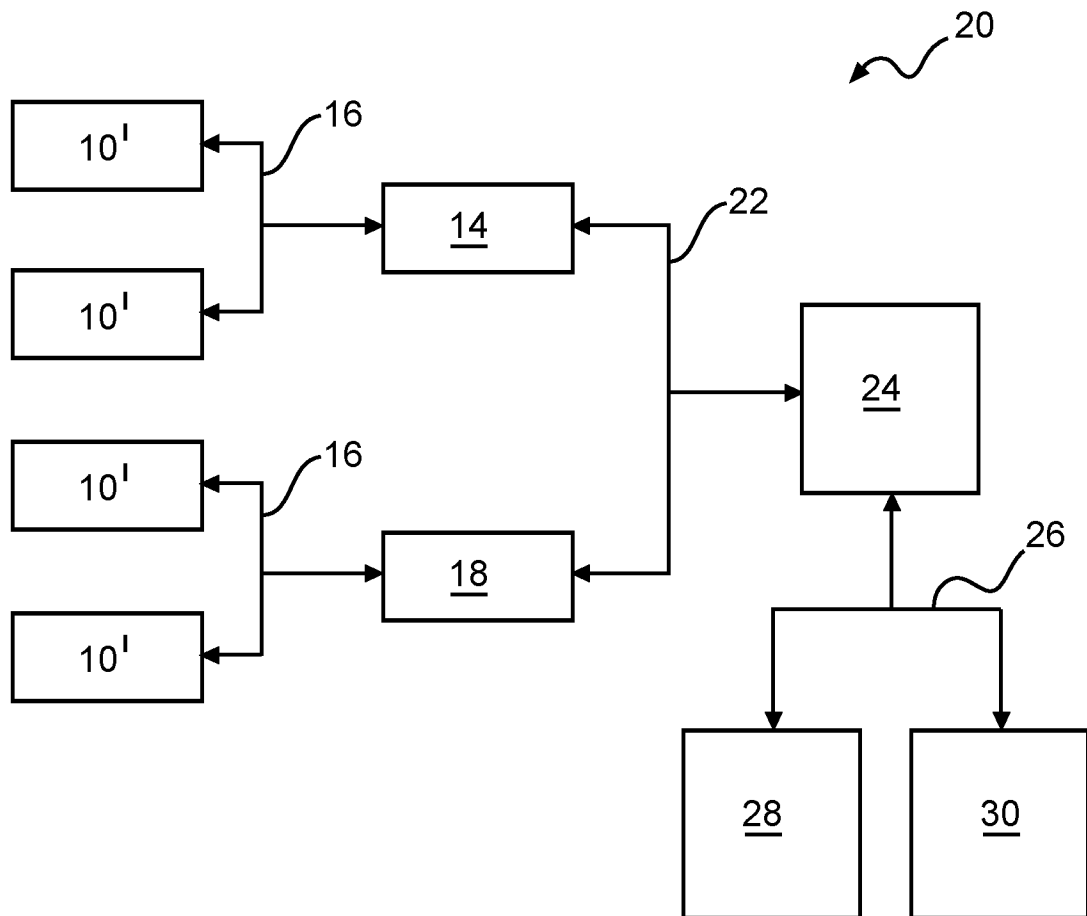


Fig. 4

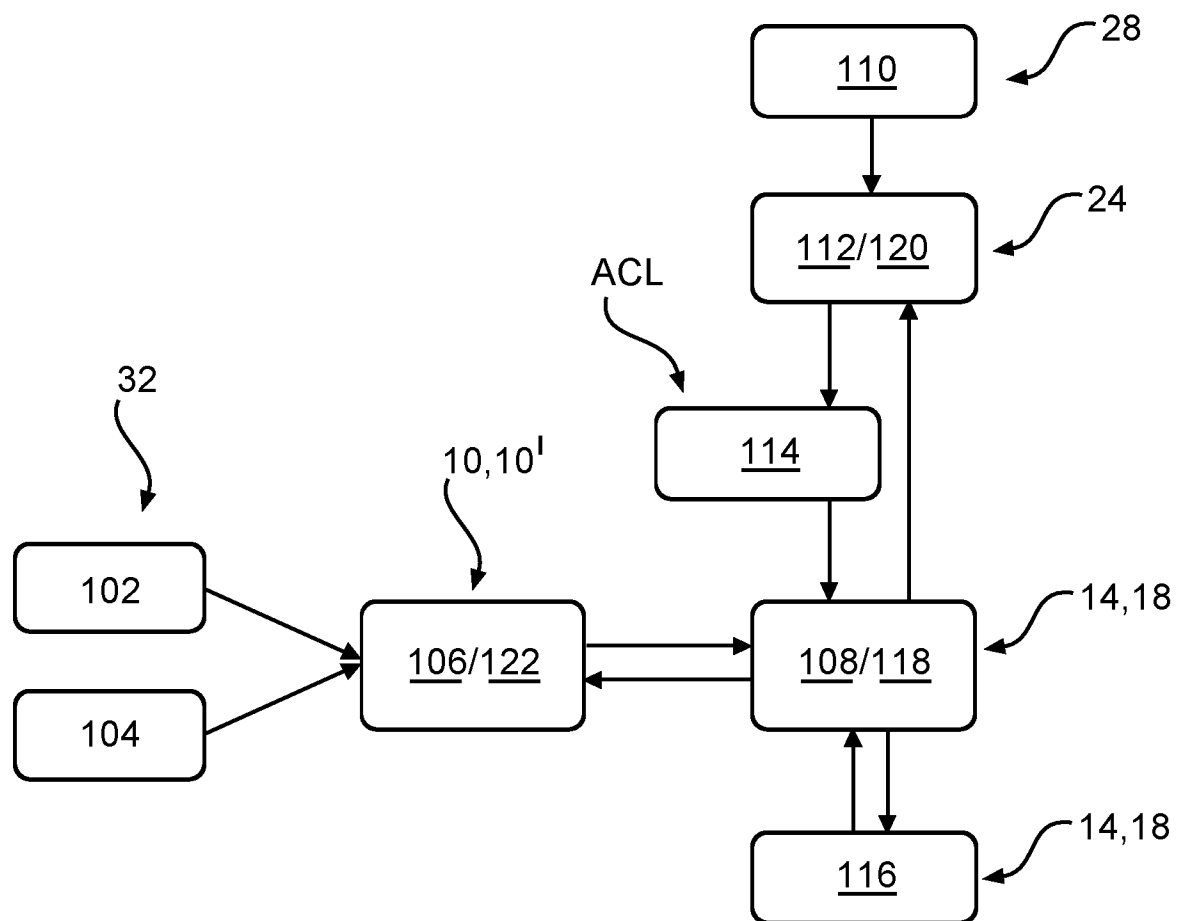


Fig. 5

4/4

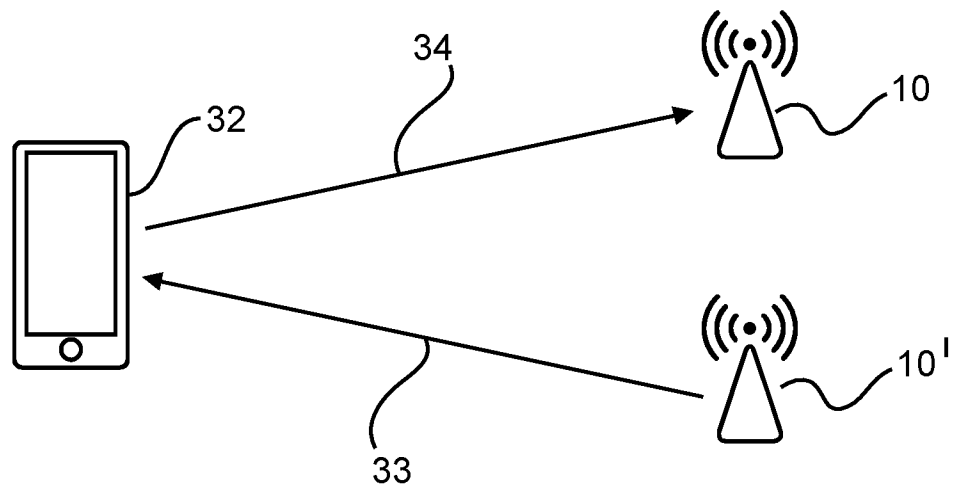


Fig. 6

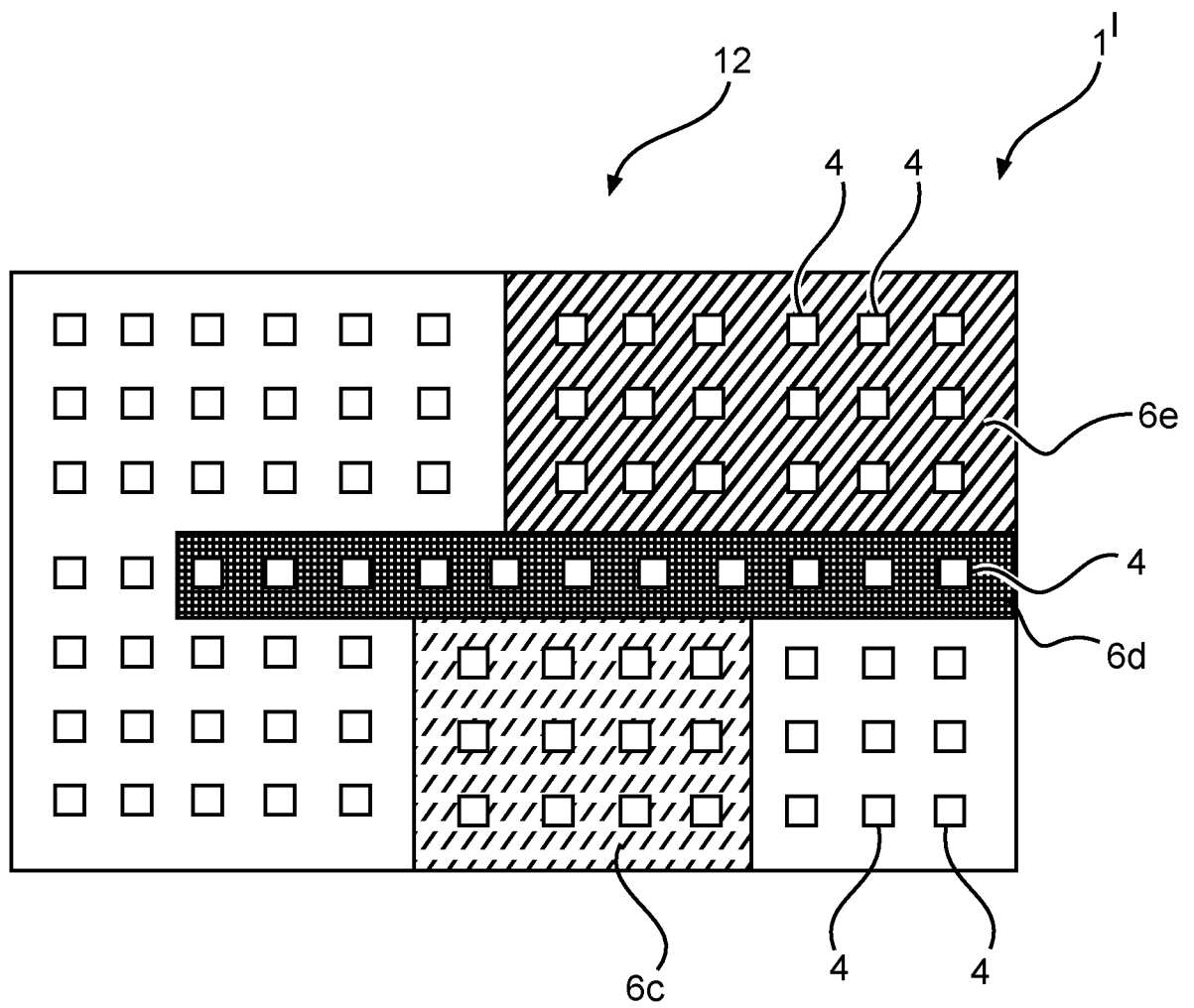


Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/EP2019/085154

A. CLASSIFICATION OF SUBJECT MATTER**H04L 29/06**(2006.01)i; **H04W 12/08**(2009.01)i; **H04W 48/04**(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2018262971 A1 (AIHARA TORU [JP] ET AL) 13 September 2018 (2018-09-13) paragraph [0021] - paragraph [0030] paragraph [0041] - paragraph [0064]; figure 2 paragraph [0074] - paragraph [0079] paragraph [0088] - paragraph [0095] paragraph [0189] - paragraph [0212]; figures 6a, 6b	1, 14 2
X A	US 2014331272 A1 (GUPTA RAJARSHI [US] ET AL) 06 November 2014 (2014-11-06) paragraph [0004] - paragraph [0018] paragraph [0053] - paragraph [0061]; figure 1 paragraph [0080] - paragraph [0095]	1, 14 2
Y	US 2012218978 A1 (ISHIDOSHIRO TAKASHI [JP]) 30 August 2012 (2012-08-30) paragraphs [0009], [0020]	2



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

25 March 2020

Date of mailing of the international search report

24 June 2020

Name and mailing address of the ISA/EP

European Patent Office
p.b. 5818, Patentlaan 2, 2280 HV Rijswijk
Netherlands

Telephone No. (+31-70)340-2040

Facsimile No. (+31-70)340-3016

Authorized officer

Raible, Markus

Telephone No.

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. claims: 1, 2, 14

The technical feature of dependent claim 2 that constitutes the difference from the non-inventive common subject matter (claim 1) consists in each of the plurality of wireless access points being allocated to a specific light fixture in the building or edifice and having a joint power supply together with said light fixture. The technical effect of this feature consists in the access points and light fixtures having a joint power supply, thereby dispensing with the need for separate, multiple resources for power supply. Hence, this feature solves the technical problem of how to be able to integrate access points into a building infrastructure to save resources.

2. claims: 3-5 (in full); 12 (in part)

The only clear feature that can be used to determine the technical effect or the problem to be solved consists in the position and movement of a terminal that registers in the network being continuously trackable throughout the building or edifice as an allocation of the terminal to the wireless access points of the grid-type network changes over time. The technical effect of this feature consists in an allocation, which changes over time, of a terminal to wireless access points in a network being evaluated in order to determine a movement of said terminal. Hence, this feature solves the technical problem of how to be able to determine the movement of a terminal in a building or edifice.

3. claims: 6, 7

Claims 6 and 7 are linked by the common technical feature "a specific hardware address of the terminal ascertained on the basis of the information received about the terminal". The technical effect of this feature consists in the selection of suitable information about a terminal, i.e. a hardware address of the terminal. This solves the technical problem of how to be able to establish suitable information about a terminal that can be used as a criterion to prevent access to a network.

4. claim: 8 (in full); 12 (in part)

Claim 8 specifies the special technical features whereby the one or more room zone controllers are designed to switch the connected wireless access points into a monitoring mode in order to operate same as WLAN sniffers for detecting external wireless access points and determining the spatial position thereof. Insofar as the features of claim 8 are clear, they appear to have the technical effect of operating the system in a mode that differs from the mode specified in main claim 1, i.e. in a monitoring mode as a WLAN sniffer. These features specify the technical problem of how to be able to detect an external wireless access point.

5. claim: 9

Claim 9 specifies the additional feature of a notification device which is connected to the security controller and/or the room zone controller and which, in the event of unauthorized network access by the terminal and/or the external access point as determined by the comparison, issues an alert message containing the time of unauthorized network access, the hardware address and the position of the terminal and/or the external access point. The technical effect of this feature consists in the generation of an alert when violations of security measures are ascertained. This solves the technical problem of how to enable the operator of a security-critical system to ascertain violations of safety measures and take precautions thereagainst.

6. claims: 10, 11, 13 (in full); 12 (in part)

Claims 10 and 13 are linked by the common technical feature of output adjustment for specific access points. This common technical feature has the technical effect of making it possible to adjust the output of an access point as a function of external conditions. This common technical feature solves the technical problem of how to be able to adjust power consumption and interference radiation in a wireless network according to the situation.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/EP2019/085154

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.: **1, 2, 14**

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/EP2019/085154

Patent document cited in search report				Publication date (day/month/year)			Patent family member(s)				Publication date (day/month/year)		
US	2018262971	A1	13 September 2018	US	2018262971	A1	13 September 2018	US	2019028956	A1	24 January 2019		
US	2014331272	A1	06 November 2014	CN	105165044	A	16 December 2015	EP	2992697	A1	09 March 2016		
				JP	2016523028	A	04 August 2016	KR	20160003177	A	08 January 2016		
				US	2014331272	A1	06 November 2014	WO	2014179152	A1	06 November 2014		
US	2012218978	A1	30 August 2012	CN	102469623	A	23 May 2012	JP	2012100027	A	24 May 2012		
				US	2012218978	A1	30 August 2012						

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP2019/085154

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L29/06 H04W12/08 H04W48/04
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherhierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L H04W

Recherhierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherhierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EP0-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2018/262971 A1 (AIHARA TORU [JP] ET AL) 13. September 2018 (2018-09-13)	1,14
Y	Absatz [0021] - Absatz [0030] Absatz [0041] - Absatz [0064]; Abbildung 2 Absatz [0074] - Absatz [0079] Absatz [0088] - Absatz [0095] Absatz [0189] - Absatz [0212]; Abbildungen 6a,6b	2
X	US 2014/331272 A1 (GUPTA RAJARSHI [US] ET AL) 6. November 2014 (2014-11-06)	1,14
A	Absatz [0004] - Absatz [0018] Absatz [0053] - Absatz [0061]; Abbildung 1 Absatz [0080] - Absatz [0095]	2
Y	US 2012/218978 A1 (ISHIDOSHIRO TAKASHI [JP]) 30. August 2012 (2012-08-30) Absätze [0009], [0020]	2

☐

Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒

Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

25. März 2020

Absenddatum des internationalen Recherchenberichts

24/06/2020

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Raible, Markus

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2019/085154

Feld Nr. II Bemerkungen zu den Ansprüchen, die sich als nicht recherchierbar erwiesen haben (Fortsetzung von Punkt 2 auf Blatt 1)

Gemäß Artikel 17(2)a) wurde aus folgenden Gründen für bestimmte Ansprüche kein internationaler Recherchenbericht erstellt:

1. ☐ Ansprüche Nr.
weil sie sich auf Gegenstände beziehen, zu deren Recherche diese Behörde nicht verpflichtet ist, nämlich
2. ☐ Ansprüche Nr.
weil sie sich auf Teile der internationalen Anmeldung beziehen, die den vorgeschriebenen Anforderungen so wenig entsprechen, dass eine sinnvolle internationale Recherche nicht durchgeführt werden kann, nämlich
3. ☐ Ansprüche Nr.
weil es sich dabei um abhängige Ansprüche handelt, die nicht entsprechend Satz 2 und 3 der Regel 6.4 a) abgefasst sind.

Feld Nr. III Bemerkungen bei mangelnder Einheitlichkeit der Erfindung (Fortsetzung von Punkt 3 auf Blatt 1)

Diese Internationale Recherchenbehörde hat festgestellt, dass diese internationale Anmeldung mehrere Erfindungen enthält:

siehe Zusatzblatt

1. ☐ Da der Anmelder alle erforderlichen zusätzlichen Recherchegebühren rechtzeitig entrichtet hat, erstreckt sich dieser internationale Recherchenbericht auf alle recherchierbaren Ansprüche.
2. ☐ Da für alle recherchierbaren Ansprüche die Recherche ohne einen Arbeitsaufwand durchgeführt werden konnte, der zusätzliche Recherchegebühr gerechtfertigt hätte, hat die Behörde nicht zur Zahlung solcher Gebühren aufgefordert.
3. ☐ Da der Anmelder nur einige der erforderlichen zusätzlichen Recherchegebühren rechtzeitig entrichtet hat, erstreckt sich dieser internationale Recherchenbericht nur auf die Ansprüche, für die Gebühren entrichtet worden sind, nämlich auf die Ansprüche Nr.
4. ☒ Der Anmelder hat die erforderlichen zusätzlichen Recherchegebühren nicht rechtzeitig entrichtet. Dieser internationale Recherchenbericht beschränkt sich daher auf die in den Ansprüchen zuerst erwähnte Erfindung; diese ist in folgenden Ansprüchen erfasst:
1, 2, 14

Bemerkungen hinsichtlich eines Widerspruchs

- ☐ Der Anmelder hat die zusätzlichen Recherchegebühren unter Widerspruch entrichtet und die gegebenenfalls erforderliche Widerspruchsgebühr gezahlt.
- ☐ Die zusätzlichen Recherchegebühren wurden vom Anmelder unter Widerspruch gezahlt, jedoch wurde die entsprechende Widerspruchsgebühr nicht innerhalb der in der Aufforderung angegebenen Frist entrichtet.
- ☐ Die Zahlung der zusätzlichen Recherchegebühren erfolgte ohne Widerspruch.

WEITERE ANGABEN

PCT/ISA/ 210

Die internationale Recherchenbehörde hat festgestellt, dass diese internationale Anmeldung mehrere (Gruppen von) Erfindungen enthält, nämlich:

1. Ansprüche: 1, 2, 14

Das technische Merkmal des abhängigen Anspruchs 2 dieser Gruppe, welches den Unterschied zum nicht-erfinderischen gemeinsamen Gegenstand (Anspruch 1) ausmacht, besteht darin dass die drahtlosen Zugangspunkte der Vielzahl jeweils einer Leuchte in dem Gebäude oder der baulichen Anlage zugeordnet sind und jeweils mit dieser eine gemeinsame Leistungsversorgung besitzen.

Die technische Wirkung des Merkmals besteht darin, dass Zugangspunkte und Leuchten eine gemeinsame Leistungsversorgung besitzen und daher Ressourcen in Bezug auf die Leistungsversorgung nicht separat bzw. mehrfach vorhanden sein müssen.

Das Merkmal löst demnach die technische Aufgabe, wie Zugangspunkte ressourcensparend in eine Gebäudeinfrastruktur eingebettet werden können.

2. Ansprüche: 3-5(vollständig); 12(teilweise)

Das einzige klare Merkmal, das zur Bestimmung der technischen Wirkung bzw. der zu lösenden Aufgabe herangezogen werden kann, besteht darin, dass im Fall eines sich im Netzwerk anmeldenden Endgeräts anhand einer sich zeitlich verändernden Zuordnung zu den drahtlosen Zugangspunkten des gitterartigen Netzes dessen Position und Bewegung im Gebäude oder der baulichen Anlage lückenlos verfolgbar ist.

Die technische Wirkung des Merkmals besteht in der Auswertung einer sich zeitlich verändernden Zuordnung eines Endgeräts zu drahtlosen Zugangspunkten eines Netzes zur Bestimmung einer Bewegung.

Das Merkmal löst demnach die technische Aufgabe, wie die Bewegung eines Endgeräts in einem Gebäude oder einer baulichen Anlage bestimmt werden kann.

3. Ansprüche: 6, 7

Die Ansprüche 6 und 7 sind durch das gemeinsame technische Merkmal "einer aus der empfangenen Geräteinformation bestimmten spezifischen Hardware-Adresse des Endgeräts" verbunden.

Die technische Wirkung dieses Merkmals besteht in der Auswahl einer geeigneten Geräteinformation eines Endgeräts, nämlich einer Hardware-Adresse des Endgeräts.

Dies löst die technische Aufgabe, wie eine geeignete Geräteinformation festgelegt werden kann, die als Kriterium zum Verhindern eines Netzzugangs herangezogen werden kann.

4. Ansprüche: 8(vollständig); 12(teilweise)

Anspruch 8 spezifiziert die besonderen technischen Merkmale, dass der oder die Raumzonencontroller ausgelegt sind, die verbundenen drahtlosen Zugangspunkte in einen Monitormodus zu schalten, um diese als WLAN-Sniffer zu betreiben, um die externen drahtlosen Zugangspunkte aufzuspüren und deren räumliche Position zu bestimmen.

Soweit die Merkmale des Anspruchs 8 klar sind, scheinen sie den technischen Effekt zu haben, dass das System in einem Modus betrieben wird, der von dem im zugrunde liegenden Anspruch 1 spezifizierten Modus abweicht, nämlich in einem Monitormodus als WLAN-Sniffer.

Die Merkmale spezifizieren die technische Aufgabe, wie ein externer drahtloser Zugangspunkt aufgespürt werden kann.

5. Anspruch: 9

Anspruch 9 spezifiziert das zusätzliche Merkmal einer Benachrichtigungsvorrichtung, die mit dem Sicherheitscontroller und/oder dem Raumzonencontroller verbunden ist und im Fall eines aus dem Vergleich resultierenden nicht autorisierten Netzzugang durch das Endgerät und/oder den externen Zugangspunkt eine Warnmeldung ausgibt, die den Zeitpunkt des nicht aut[orisierten] Netzzugangs, die Hardware-Adresse und die Position des Endgeräts und/oder des externen Zugangspunkts beinhaltet. Die technische Wirkung dieses Merkmals besteht in der Erzeugung einer Warnung, wenn Verstöße gegen Sicherheitsmaßnahmen festgestellt werden .

Dies löst die technische Aufgabe, wie der Betreiber eines sicherheitskritischen Systems in die Lage versetzt werden kann, Verstöße gegen Sicherheitsmaßnahmen festzustellen und Maßnahmen dagegen zu ergreifen.

6. Ansprüche: 10, 11, 13(vollständig); 12(teilweise)

Die Ansprüche 10 und 13 sind durch das gemeinsame technische Merkmal einer Leistungseinstellung für bestimmte Zugangspunkte verbunden.

Dieses gemeinsame technische Merkmal bewirkt den technischen Effekt, dass die Leistung eines Zugangspunkt in Abhängigkeit von externen Bedingungen eingestellt werden kann.

Das gemeinsame technische Merkmal löst die technische Aufgabe, wie der Energieverbrauch und die Störabstrahlung eines drahtlosen Netzwerks situationsabhängig angepasst werden kann.

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2019/085154

Im Recherchenbericht angeführtes Patentdokument			Datum der Veröffentlichung		Mitglied(er) der Patentfamilie		Datum der Veröffentlichung	
US 2018262971	A1	13-09-2018	US	2018262971	A1	13-09-2018		
US 2014331272	A1	06-11-2014	US	2019028956	A1	24-01-2019		
US 2014331272	A1	06-11-2014	CN	105165044	A	16-12-2015		
US 2014331272	A1	06-11-2014	EP	2992697	A1	09-03-2016		
US 2014331272	A1	06-11-2014	JP	2016523028	A	04-08-2016		
US 2014331272	A1	06-11-2014	KR	20160003177	A	08-01-2016		
US 2014331272	A1	06-11-2014	US	2014331272	A1	06-11-2014		
US 2014179152	A1	06-11-2014	WO	2014179152	A1	06-11-2014		
US 2012218978	A1	30-08-2012	CN	102469623	A	23-05-2012		
US 2012218978	A1	30-08-2012	JP	2012100027	A	24-05-2012		
US 2012218978	A1	30-08-2012	US	2012218978	A1	30-08-2012		