

(12)

Patentschrift

- (21) Anmeldenummer: A 1377/2006 (51) Int. Cl.⁸: **G01S 1/68** (2006.01)
H04Q 7/38 (2006.01)
(22) Anmeldetag: 2006-08-16
(43) Veröffentlicht am: 2008-03-15

(56) Entgegenhaltungen:
GB 2535910A WO 2005/106523A1

(73) Patentanmelder:
FTW. FORSCHUNGSZENTRUM
TELEKOMMUNIKATION
WIEN BETRIEBS-GMBH
A-1220 WIEN (AT)

(72) Erfinder:
BESSLER SANDFORD DIPL.ING. DR.
WIEN (AT)

(54) VERFAHREN UND ANLAGE ZUM GEBIETSWEISEN LOKALISIEREN VON TARGETS

- (57) Verfahren zum gebietsweisen Lokalisieren von Targets, die jeweils mit einem Transponder (1) versehen sind, dessen Reichweite auf ein Gebiet (2) beschränkt ist und der eine eindeutige Targetkennung (u_i) enthält, mit Hilfe von den Gebieten zugeordneten Funkbaken (3) zum Ansprechen der jeweils in einem Gebiet anwesenden Transponder, wobei in jeder Funkbake (3) periodisch die Targetkennungen der anwesenden Transponder (1) abgerufen werden, wobei jede von einer Funkbake (3) abgerufene Targetkennung mit einer eindeutigen Gebietskennung (b_j) dieser Funkbake (3) zu einem Verschlüsselungswert ($H(u_i, b_j)$) verschlüsselt wird, wobei jeder Verschlüsselungswert ($H(u_i, b_j)$) für eine vorbestimmte Zeitspanne (T) in einer Datenbank (6) zur Abfrage bereitgestellt wird, und wobei für eine Abfrage der Datenbank (6) eine gesuchte Targetkennung mit einer angefragten Gebietskennung verschlüsselt ($reqH(u_i, b_j)$) und mit den bereitgestellten Verschlüsselungswerten ($H(u_i, b_j)$) verglichen und im Gleichheitsfall das gesuchte Target als im angefragten Gebiet anwesend gemeldet wird.

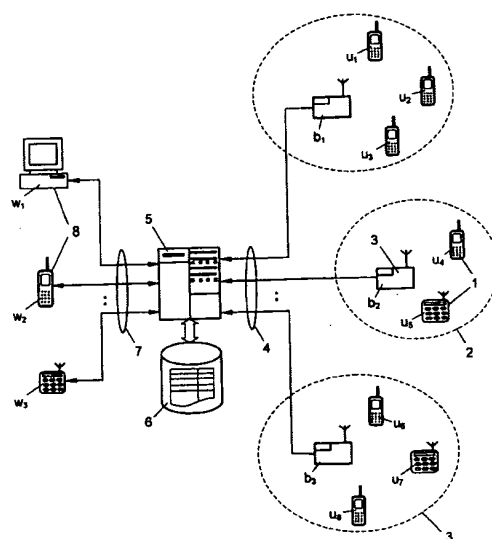


Fig. 1

Die vorliegende Erfindung betrifft ein Verfahren und eine Anlage zum gebietsweisen Lokalisieren von Targets, die jeweils mit einem Transponder versehen sind, dessen Reichweite auf ein Gebiet beschränkt ist und der eine eindeutige Targetkennung enthält, mit Hilfe von den Gebieten zugeordneten Funkbaken zum Ansprechen der jeweils in einem Gebiet anwesenden Transponder.

Die bekannten Systeme zum Lokalisieren von Targets, beispielsweise Teilnehmern mit Mobiltelefonen in einem Telekommunikationsnetz, erfordern aus Datenschutzgründen stets eine aufrechte Registrierungsbeziehung („Subscription“) zwischen der anfragenden Einheit („Watcher“) und dem Target. Damit ist eine Lokalisierung von Targets durch anonyme Beobachter nicht möglich; würden diese zugelassen, wäre die Privatsphäre des Targets, z.B. einer gesuchten Person, empfindlich gestört.

Es besteht daher ein Bedarf nach Verfahren und Anlagen zum Lokalisieren von Targets, welche einerseits einen anonymen Betrieb ermöglichen, um breite Akzeptanz für neue Anwendungsgebiete zu erhalten, die aber andererseits ausreichenden Schutz der Privatsphäre der teilnehmenden Benutzer bieten.

Dieses Ziel wird in einem ersten Aspekt mit einem Verfahren der einleitend genannten Art erreicht, das sich gemäß der Erfindung dadurch auszeichnet,

daß in jeder Funkbake periodisch die Targetkennungen der anwesenden Transponder abgerufen werden,

daß jede von einer Funkbake abgerufene Targetkennung mit einer eindeutigen Gebietskennung dieser Funkbake zu einem Verschlüsselungswert verschlüsselt wird, und

daß jeder Verschlüsselungswert für eine vorbestimmte Zeitspanne in einer Datenbank zur Abfrage bereitgestellt wird,

wobei für eine Abfrage der Datenbank eine gesuchte Targetkennung mit einer angefragten Gebietskennung verschlüsselt und mit den bereitgestellten Verschlüsselungswerten verglichen und im Gleichheitsfall das gesuchte Target als im angefragten Gebiet anwesend gemeldet wird.

Auf diese Weise wird es erstmals möglich, einen anonymen, gebietsweisen Lokalisierungsdienst zur Verfügung zu stellen, der gleichzeitig einen ausreichenden Schutz der Privatsphäre der lokalisierten Teilnehmer bietet: In der abfragbaren Datenbank liegen die Targetkennungen nur in - von unterschiedlichen Funkbaken unterschiedlich - verschlüsselter Form vor, so daß sich selbst aus einer mißbräuchlichen Auswertung der gesamten Datenbank keine Bewegungsprofile der Targets erstellen ließen. Die Lokalisierung eines Targets ist nur möglich, wenn sowohl die Targetkennung als auch die Gebietskennung bekannt sind, d.h. das Verfahren gestattet keine weitergehende Abfrage als jene, ob eine bestimmte, gesuchte Targetkennung in einem bestimmten, angefragten Gebiet gerade - bzw. innerhalb der letzten vorbestimmten Zeitspanne - anwesend ist oder war. Die Abfrage ist an keine weiteren Bedingungen als die Kenntnis der Target- und Gebietskennung geknüpft und in diesem Sinne „anonym“ möglich, d.h. ohne Registrierungsbeziehung oder Rückfrage beim Target.

Die Erfindung schafft damit völlig neue Anwendungsgebiete, die es einem anfragenden Benutzer (Watcher) ermöglichen, das aktuelle Aufenthaltsgebiet anderer Benutzer (Targets), die ihm ihre Target- und möglichen Gebietskennungen zur Verfügung stellen, festzustellen. Gleichzeitig ist der Schutz der Privatsphäre gegenüber Dritten, welche die Target- und Gebietskennungen nicht kennen, gewährleistet.

Das Verfahren der Erfindung ist darüber hinaus ausgezeichnet skalierbar, da der gerätetechnische Aufwand nur linear mit der Anzahl der Gebiete steigt. Für die Kommunikation zwischen den Funkbaken und der Datenbank genügt eine einfache Einwegekommunikation, was den Hardwareaufwand für die Funkbaken stark reduziert.

Eine erste bevorzugte Ausführungsform der Erfindung zeichnet sich dadurch aus, daß die Targetkennungen von den Funkbaken periodisch an einen zentralen Server gesendet werden, welcher diese mit den jeweiligen Gebietskennungen verschlüsselt und für die genannte Zeitspanne in die Datenbank einträgt, was den Aufwand in den Funkbaken noch weiter reduziert.

Alternativ können bevorzugt die Targetkennungen von den Funkbaken mit ihren jeweiligen Gebietskennungen verschlüsselt und periodisch an einen zentralen Server gesendet werden, welcher die empfangenen Verschlüsselungswerte für die genannte Zeitspanne in die Datenbank einträgt. Dies hat den Vorteil, daß die Funkbaken bereits verschlüsselte Codes an den Server senden, sodaß selbst ein Abhören des Meldungsverkehrs zwischen den Funkbaken und dem Server keinen Aufschluß über die Targets gibt.

Gemäß einem weiteren bevorzugten Merkmal der Erfindung wird zur Verschlüsselung ein Hash-Algorithmus verwendet. Dies stellt eine besonders einfache, für den genannten Zweck ausreichend sichere Art der Verschlüsselung der Target- und Gebietskennungen dar.

Besonders vorteilhaft ist es, wenn gemäß einem weiteren Merkmal der Erfindung die Funkbaken und Transponder untereinander nach dem Bluetooth-Standard kommunizieren. Bluetooth® ist ein proprietärer Industriestandard der Bluetooth SIG Inc. zur digitalen Kurzreichweiten-Kommunikation (digital short range communication, DSRC) und aufgrund seiner begrenzten Reichweite besonders geeignet. Bevorzugt werden bluetooth-fähige Mobiltelefone als Transponder verwendet.

Eine weitere vorteilhafte Ausführungsform der Erfindung zeichnet sich dadurch aus, daß der Server die Datenbank über das Internet zur Abfrage bereitstellt. Dadurch ist eine weltweite Abfrage und Lokalisierung möglich.

In einem weiteren Aspekt schafft die Erfindung eine Anlage zum gebietsweisen Lokalisieren von Targets wie in den Ansprüchen 6 bis 10 definiert. Bezüglich der Merkmale und Vorteile der erfindungsgemäßen Anlage wird auf die obigen Ausführungen zum Verfahren verwiesen.

Die Erfindung wird nachstehend anhand eines in den beigeschlossenen Zeichnungen dargestellten Ausführungsbeispiels näher erläutert. In den Zeichnungen zeigt;

Fig. 1 ein Blockschaltbild der Anlage der Erfindung;
Fig. 2 den Aufbau der Datenbank am Server;
Fig. 3 ein Sequenzdiagramm einer ersten Variante des Verfahrens der Erfindung; und
Fig. 4 ein Sequenzdiagramm einer zweiten Variante des Verfahrens der Erfindung.

Fig. 1 zeigt eine Anlage zum Lokalisieren von Targets mit Transpondern 1, die sich jeweils im Bedeckungsgebiet 2 einer Funkbake 3 befinden. Die Grenze jedes Gebietes 2 ergibt sich aus der begrenzten Reichweite der Transponder 1 bei ihrer Funkkommunikation mit der Funkbake 3 des Gebietes 2.

Wie in Fig. 1 gezeigt, können die Transponder 1 beliebiger Art sein, beispielsweise Mobiltelefone, PDAs, RFID-Chips, usw.

Die Funkverbindung zwischen Transpondern 1 und Funkbaken 3 erfolgt bevorzugt nach dem Bluetooth-Standard, welcher aufgrund der kurzen Reichweite kleine Gebiete 2 und damit eine genauere Lokalisierung ergibt; alternativ können beliebige andere Arten von Kurzreichweiten-Funkverbindungen verwendet werden, beispielsweise solche zum Auslesen von RFID-Chips.

Die Transponder 1 enthalten jeweils eine eindeutige Targetkennung u_i (hier: $i = 1..8$) welche über die Funkverbindung auslesbar bzw. abfragbar ist. Die Funkbaken 3 enthalten ihrerseits eine eindeutige Gebietskennung b_j (hier: $j = 1..3$).

Die Funkbaken 3 stehen über Datenverbindungen 4, beispielsweise Internet-, Telefon- oder Mobilfunkkanäle, mit einem zentralen Server 5 in Verbindung. Die Funkbaken 3 übermitteln periodisch die Targetkennungen u_i aller in ihrem Gebiet 2 aktuell anwesenden Transponder 1, jeweils verschlüsselt mit ihrer Gebietskennungen b_j , an den Server 5. Der Server 5 trägt die empfangenen Verschlüsselungswerte $H(u_i, b_j)$ in eine Datenbank 6 zur öffentlichen Abfrage ein. Alternativ kann die Verschlüsselung auch erst am Server 5 erfolgen, wie nachstehend noch ausführlicher erläutert wird.

Die Abfrage der Datenbank 6 erfolgt über eine beliebige Datenverbindung 7, beispielsweise Internet-, Telefon- oder Mobilfunkkanäle, von beliebigen Endgeräten 8 aus, z.B. PCs, Mobiltelefonen, PDAs, usw., hier mit den Kennungen w_1, w_2, w_3 .

Bei der Abfrage werden die Targetkennung u_i eines gesuchten Targets 1 und die Gebietskennung b_j eines angefragten Gebiets 2 verschlüsselt - u.zw. in derselben Weise wie zuvor von den Funkbaken 3 verschlüsselt - über die Datenverbindung 7 an den Server 5 gesandt. Der Server 5 vergleicht einen angefragten Verschlüsselungswert $reqH(u_i, b_j)$ mit den in der Datenbank 6 gespeicherten Verschlüsselungswerten $H(u_i, b_j)$ und meldet im Übereinstimmungsfall die gesuchte Targetkennung u_i als im Gebiet b_j anwesend an Endgerät 8 zurück.

Der Server 5 löscht in regelmäßigen Abständen alte Einträge $H(u_i, b_j)$ aus der Datenbank 6. Zu diesem Zweck wird jeder Eintrag $H(u_i, b_j)$ mit einem Zeitstempel t_n (hier: $n = a, b, \dots$) usw. über Datum und Zeit seines Eintragens in die Datenbank 6 versehen, wie aus Fig. 2 ersichtlich. Einträge in der Datenbank 6, deren Zeitstempel t_n älter als eine vorbestimmte Zeitspanne T ist, z.B. 5 min, werden gelöscht.

Dadurch, daß die von allen Funkbaken 3 einlangenden Verschlüsselungswerte $H(u_i, b_j)$ in einer einzigen gemeinsamen Datenbank 6 gehalten werden, ist sichergestellt, daß aus den verschlüsselten Einträgen keine Rückschlüsse auf die Funkbaken gezogen und damit keine Bewegungsprofile der Targets abgeleitet werden können: In der Datenbank 6 werden für neu in einem Gebiet 2 auftretende Targets 1 neue Einträge $H(u_i, b_j)$ eingefügt, für in einem Gebiet 2 bleibende Targets 1 werden die bestehenden Einträge $H(u_i, b_j)$ überschrieben, und für Targets 1, die nicht mehr im Gebiet 2 einer Funkbake 3 sind, werden die Einträge $H(u_i, b_j)$ auf Basis des Zeitstempels t_n bei Überschreiten der Zeitspanne T gelöscht.

Die Zeitspanne T , für welche die Einträge in der Datenbank 6 belassen werden, ist bevorzugt an die Periodizität der Sendungen der Funkbaken 3 angepaßt, um eine bestimmte zeitliche Auflösung zu erreichen: Beispielsweise sendet jede Funkbake 3 alle 5 min die Verschlüsselungswerte $H(u_i, b_j)$ der anwesenden Targets 1 an den Server 5, und Einträge $H(u_i, b_j)$ in der Datenbank 6, die älter als 5 min sind, werden im selben Rhythmus aus der Datenbank 6 gelöscht.

Fig. 3 zeigt den Ablauf einer ersten beispielhaften Ausführungsform des Verfahrens im Detail anhand der Funkbake 3 mit der Kennung b_2 , zwei beispielhaften Transpondern 1 mit den Kennungen u_4 und u_5 und einem, anfragenden Endgerät 8 mit der Kennung w_2 .

Im gezeigten Beispiel tritt die Targetkennung u_5 zu einem ersten Zeitpunkt t_1 in das Gebiet b_2 ein; zu einem weiteren Zeitpunkt t_2 die Targetkennung u_4 ; zu einem Zeitpunkt t_3 verläßt die Targetkennung u_4 wieder das Gebiet b_2 ; und zu einem Zeitpunkt t_4 verläßt auch die Targetkennung u_5 wieder das Gebiet b_2 .

Durch periodisches Abfragen (9) der in ihrem Gebiet 2 befindlichen Transponder 1 verfügt jede Funkbake 3 über die Targetkennungen u_i aller sich in ihrem Gebiet 2 befindlichen Transponder 1. In periodischen Sendungen (10) übermittelt jede Funkbake 3 die Verschlüsselungswerte $H(u_i, b_j)$ für alle anwesenden Transponder 1 an den Server 5, das sind im gezeigten Beispiel vor dem Zeitpunkt t_1 keine; nach dem Zeitpunkt t_2 die Werte $[H(u_4, b_2), H(u_5, b_2)]$; und zwischen t_3

und t_4 der Wert $[H(u_5, b_2)]$.

Der Server 5 trägt die empfangenen Verschlüsselungswerte $H(u_i, b_j)$ mit entsprechenden Zeitstempeln t_n in die Datenbank 6 ein (Fig. 2).

5

Zu einem zwischen t_3 und t_4 liegenden Zeitpunkt sendet das Endgerät w_2 eine Lokalisierungsanfrage (11) an den Server 5, welche sich aus einer gesuchten Targetkennung u_4 und einer angefragten Gebietskennung b_2 zusammensetzt, und zwar in der gleichen Weise zu einem angefragten Verschlüsselungswert $reqH(u_4, b_2)$ verschlüsselt. Der Server 5 antwortet darauf mit „Ja“ an das abfragende Endgerät w_2 .

10

Das Beispiel in Fig. 3 zeigt, daß die Lokalisierung mit einer zeitlichen Unschärfe behaftet ist, die um so kürzer ist, je kürzer die Intervalle der Sendungen 10 und die Behalte-Zeitspanne T in der Datenbank 6 sind.

15

Wird dieselbe Abfrage $reqH(u_4, b_2)$ nach dem Zeitpunkt t_4 durchgeführt, antwortet der Server 5 mit „Nein“ an das Endgerät w_2 .

20

Fig. 4 zeigt den Ablauf einer zweiten beispielhaften Ausführungsform des Verfahrens, wobei hier nur die Unterschiede zu dem Verfahren von Fig. 3 erläutert werden.

Bei der Verfahrensvariante von Fig. 4 senden die Funkbaken 3 periodisch die Targetkennungen $[u_i]$ der anwesenden Transponder 1 zusammen mit ihrer Gebietskennung b_j an den Server 5 (Schritt 10a), welcher anschließend jede Targetkennung u_i mit der entsprechenden Gebietskennung b_j zu dem Verschlüsselungswert $H(u_i, b_j)$ verschlüsselt und für die Zeitspanne T in die Datenbank 6 einträgt (Schritt 10b).

25

Für das Senden der unverschlüsselten Targetkennungen u_i im Schritt 10a können zusätzlich an sich bekannte kryptographische Verfahren zum Schutz gegen ein Abhören der Verbindung angewandt werden, beispielsweise secure socket layer (SSL)-Verbindungen.

30

Für die Verschlüsselung H der Target- und Gebietskennungen u_i, b_j zu den Verschlüsselungswerten $H(u_i, b_j)$ kann grundsätzlich jedes in der Technik bekannte Verschlüsselungsverfahren verwendet werden. Besonders geeignet sind alle Arten von Hash-Algorithmen (Digest-Algorithmen), welche einen - mit vertretbarem Aufwand - nicht-rückentschlüsselbaren Ausgangswert („Hash“) aus einem Eingangswert bilden. Die Tatsache, daß die Hash-Werte unterschiedlicher Eingangswerte in seltenen Fällen gleich sein können, ist in der Praxis vernachlässigbar, wenn hinreichend große Wortlängen für die Target- und Gebietskennungen verwendet werden.

35

Als Targetkennungen u_i können beliebige eindeutige Kennungen der Transponder 1 verwendet werden, beispielsweise SIM- oder IMEI-Nummern von Mobiltelefonen. Bevorzugt werden jedoch vom Benutzer frei wählbare Bluetooth-Gerätekennungen verwendet, welche der Benutzer an jene Personen seines Vertrauens weitergibt, denen er die Abfrage gestatten möchte.

40

Die Gebietskennungen b_j jener Gebiete 2, in denen der Benutzer die Feststellung seines Aufenthalts gestatten möchte, können ebenso nur bestimmten Personen zur Verfügung gestellt werden, oder die Gebietskennungen b_j werden - z.B. bei öffentlich als Feststellungsgebiete ausgewiesenen Gebieten 2 - in einer öffentlich einsehbaren Liste am Server 5 bereitgestellt.

45

Die Erfindung ist nicht auf die dargestellten Ausführungsformen beschränkt, sondern umfaßt alle Varianten und Modifikationen, die in den Rahmen der angeschlossenen Ansprüche fallen.

50

55

Patentansprüche:

1. Verfahren zum gebietsweisen Lokalisieren von Targets, die jeweils mit einem Transponder versehen sind, dessen Reichweite auf ein Gebiet beschränkt ist und der eine eindeutige Targetkennung enthält, mit Hilfe von den Gebieten zugeordneten Funkbaken zum Ansprechen der jeweils in einem Gebiet anwesenden Transponder, *dadurch gekennzeichnet*, daß in jeder Funkbake (3) periodisch die Targetkennungen der anwesenden Transponder (1) abgerufen werden, daß jede von einer Funkbake (3) abgerufene Targetkennung mit einer eindeutigen Gebietskennung (b_i) dieser Funkbake (3) zu einem Verschlüsselungswert ($H(u_i, b_i)$) verschlüsselt wird, und daß jeder Verschlüsselungswert ($H(u_i, b_i)$) für eine vorbestimmte Zeitspanne (T) in einer Datenbank (6) zur Abfrage bereitgestellt wird, wobei für eine Abfrage der Datenbank (6) eine gesuchte Targetkennung mit einer angefragten Gebietskennung verschlüsselt ($reqH(u_i, b_i)$) und mit den bereitgestellten Verschlüsselungswerten ($H(u_i, b_i)$) verglichen und im Gleichheitsfall das gesuchte Target als im angefragten Gebiet anwesend gemeldet wird.
2. Verfahren nach Anspruch 1, *dadurch gekennzeichnet*, daß die Targetkennungen (u_i) von den Funkbaken (3) periodisch an einen zentralen Server (5) gesendet werden, welcher diese mit den jeweiligen Gebietskennungen (b_i) verschlüsselt und für die genannte Zeitspanne (T) in die Datenbank (6) einträgt.
3. Verfahren nach Anspruch 1, *dadurch gekennzeichnet*, daß die Targetkennungen (u_i) von den Funkbaken (3) mit ihren jeweiligen Gebietskennungen (b_i) verschlüsselt und periodisch an einen zentralen Server (5) gesendet werden, welcher die empfangenen Verschlüsselungswerte ($H(u_i, b_i)$) für die genannte Zeitspanne (T) in die Datenbank (6) einträgt.
4. Verfahren nach einem der Ansprüche 1 bis 3, *dadurch gekennzeichnet*, daß zur Verschlüsselung ($H(u_i, b_i)$) ein Hash-Algorithmus verwendet wird.
5. Verfahren nach einem der Ansprüche 1 bis 4, *dadurch gekennzeichnet*, daß die Funkbaken (3) und Transponder (1) untereinander nach dem Bluetooth-Standard kommunizieren.
6. Anlage zum gebietsweisen Lokalisieren von Targets, wobei jedes Target mit einem Transponder (1), dessen Reichweite auf ein Gebiet (2) beschränkt ist und der eine eindeutige Targetkennung (u_i) enthält, und jedes Gebiet (2) mit einer Funkbake (3) zum Ansprechen der im Gebiet (2) anwesenden Transponder (1) ausgestattet ist, *dadurch gekennzeichnet*, daß jede Funkbake (3) periodisch die Targetkennungen (u_i) der anwesenden Transponder (1) abrufen und an einen zentralen Server (5) sendet, welcher jede empfangene Targetkennung (u_i) mit einer eindeutigen Gebietskennung (b_i) der jeweiligen Funkbake (3) verschlüsselt und den Verschlüsselungswert ($H(u_i, b_i)$) für eine vorbestimmte Zeitspanne (T) in einer Datenbank (6) zur Abfrage bereitstellt, wobei der Server (5) sich aus gesuchten Target- und angefragten Gebietskennung zusammensetzende abgefragte Verschlüsselungswerte ($reqH(u_i, b_i)$) mit den bereitgestellten Verschlüsselungswerten ($H(u_i, b_i)$) vergleicht und im Gleichheitsfall das gesuchte Target als im angefragten Gebiet anwesend meldet.
7. Anlage zum gebietsweisen Lokalisieren von Targets, wobei jedes Target mit einem Transponder (1), dessen Reichweite auf ein Gebiet (2) beschränkt ist und der eine eindeutige Targetkennung (u_i) enthält, und jedes Gebiet (2) mit einer Funkbake (3) zum Ansprechen der im Gebiet (2) anwesenden Transponder (1) ausgestattet ist, *dadurch gekennzeichnet*, daß jede Funkbake (3) periodisch die Targetkennungen (u_i) der anwesenden Transponder

(1) abrufen, mit einer eindeutigen Gebietskennung (b_i) verschlüsselt und an einen zentralen Server (5) senden,

welcher jeden empfangenen Verschlüsselungswert ($H(u_i, b_j)$) für eine vorbestimmte Zeitspanne (T) in einer Datenbank (6) zur Abfrage bereitstellt,

wobei der Server (5) sich aus gesuchten Target- und angefragten Gebietskennung zusammensetzende abgefragte Verschlüsselungswerte ($reqH(u_i, b_j)$) mit den bereitgestellten Verschlüsselungswerten ($H(u_i, b_j)$) vergleicht und im Gleichheitsfall das gesuchte Target als im angefragten Gebiet anwesend meldet.

8. Anlage nach Anspruch 6 oder 7, *dadurch gekennzeichnet*, daß als Verschlüsselung (H) ein Hash-Algorithmus dient.

9. Anlage nach einem der Ansprüche 6 bis 8, *dadurch gekennzeichnet*, daß die Funkbaken (3) und Transponder (1) untereinander nach dem Bluetooth-Standard kommunizieren.

10. Anlage nach einem der Ansprüche 6 bis 9, *dadurch gekennzeichnet*, daß der Server (5) ein Internetserver ist.

Hiezu 3 Blatt Zeichnungen

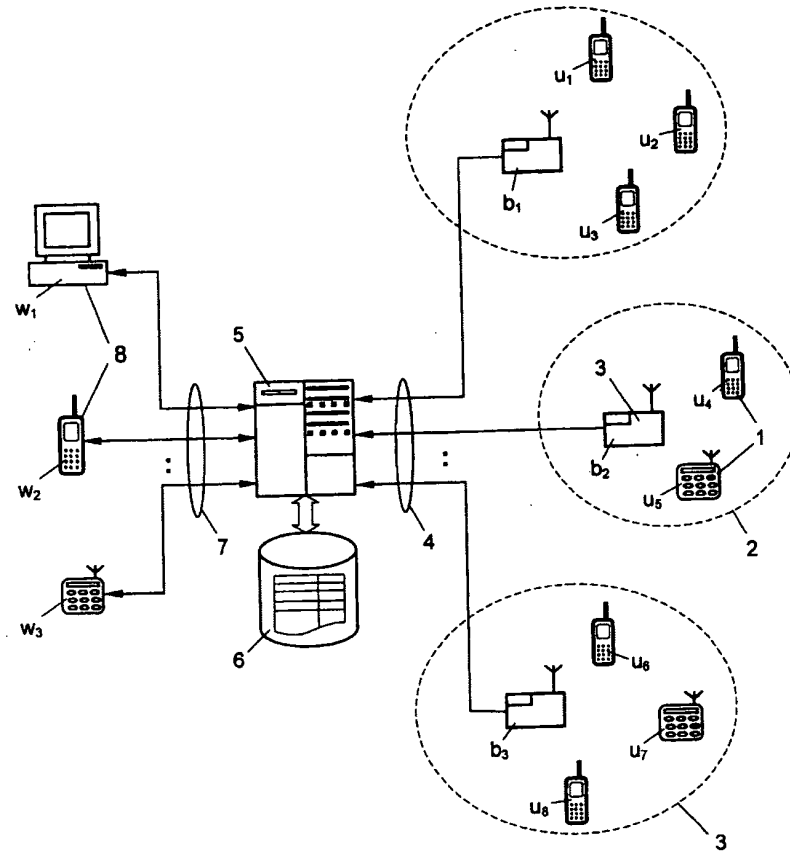


Fig. 1

$H(u_1, b_1)$	t_a
$H(u_2, b_1)$	t_b
$H(u_3, b_1)$	t_c
$H(u_4, b_2)$	t_d
$H(u_5, b_2)$	t_e
:	:
:	:

6

Fig. 2

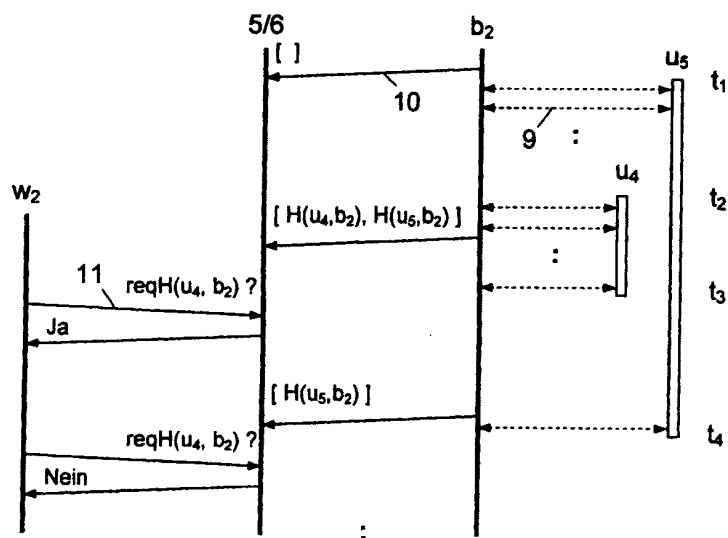


Fig. 3

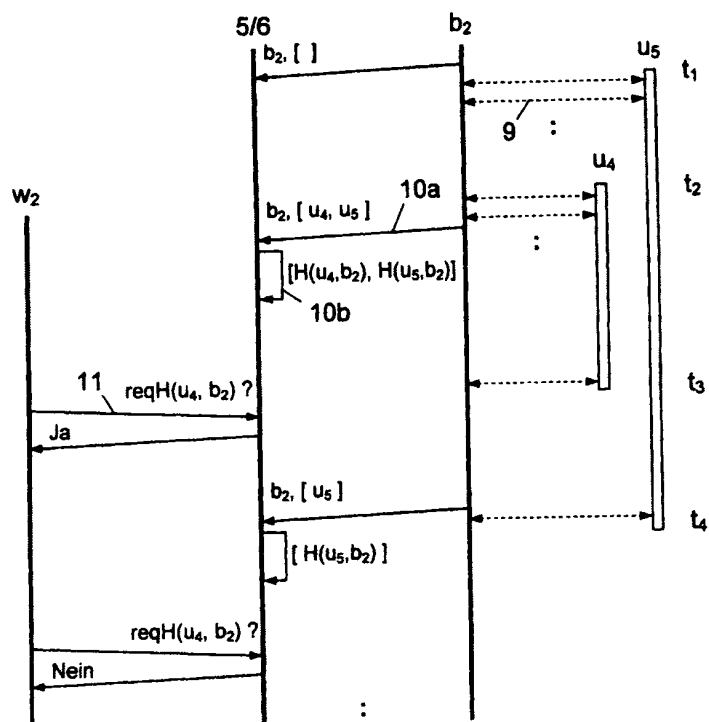


Fig. 4