



(11) **EP 1 474 786 B1**

(12) **FASCICULE DE BREVET EUROPEEN**

(45) Date de publication et mention  
de la délivrance du brevet:  
**12.12.2007 Bulletin 2007/50**

(51) Int Cl.:  
**G08B 27/00 (2006.01) G08B 26/00 (2006.01)**

(21) Numéro de dépôt: **03715051.3**

(86) Numéro de dépôt international:  
**PCT/FR2003/000250**

(22) Date de dépôt: **27.01.2003**

(87) Numéro de publication internationale:  
**WO 2003/065325 (07.08.2003 Gazette 2003/32)**

(54) **PROCEDE DE SURVEILLANCE D'UN PARC D'HORODATEURS ET HORODATEURS ADAPTES  
A CET EFFET**

VERFAHREN ZUR ÜBERWACHUNG EINES ZEITSTEMPELPARKS UND ZEITSTEMPEL DAFÜR  
METHOD FOR MONITORING A PARKING LOT WITH PARKING METERS AND CORRESPONDING  
PARKING METERS

(84) Etats contractants désignés:  
**DE ES FR GB NL**

(72) Inventeur: **MANDY, Damien**  
**F-25660 Fontain (FR)**

(30) Priorité: **29.01.2002 FR 0201069**

(74) Mandataire: **Domenego, Bertrand et al**  
**Cabinet Lavoix**  
**2, place d'Estienne d'Orves**  
**75441 Paris Cedex 09 (FR)**

(43) Date de publication de la demande:  
**10.11.2004 Bulletin 2004/46**

(73) Titulaire: **PARKEON**  
**75015 Paris (FR)**

(56) Documents cités:  
**DE-A- 19 633 861 GB-A- 2 273 593**

**EP 1 474 786 B1**

Il est rappelé que: Dans un délai de neuf mois à compter de la date de publication de la mention de la délivrance du brevet européen, toute personne peut faire opposition au brevet européen délivré, auprès de l'Office européen des brevets. L'opposition doit être formée par écrit et motivée. Elle n'est réputée formée qu'après paiement de la taxe d'opposition. (Art. 99(1) Convention sur le brevet européen).

## Description

**[0001]** L'invention concerne le domaine des dispositifs automatiques de paiement, du type terminal, borne, horodateur, mis à la disposition du public et plus particulièrement la protection de ces dispositifs contre les attaques frauduleuses.

**[0002]** Étant isolés et aptes à contenir de l'argent, ces dispositifs de paiement sont susceptibles de subir des attaques aussi bien au niveau du dispositif lui-même que de ses moyens de communication et doivent donc être équipés de moyens de dissuasion.

**[0003]** D'une manière générale ces moyens de dissuasion doivent avoir pour fonctions d'une part de détecter une éventuelle attaque et d'autre part de signaler cette attaque.

**[0004]** On connaît déjà des bornes publiques de paiement destinées à être installées dans les rues d'une ville et disposant de moyens de dissuasion contre les attaques.

**[0005]** Chacune de ces bornes connues dispose d'une connexion au réseau téléphonique et de moyens de détection d'une éventuelle attaque.

**[0006]** Lorsqu'une attaque est perpétrée contre une de ces bornes, celle-ci compose le numéro de téléphone d'un central de surveillance et lui envoie un signal d'alerte.

**[0007]** Ces bornes connues présentent un certain nombre d'inconvénients.

**[0008]** En effet, l'existence d'un tel moyen d'alerte étant connue, les fraudeurs tendent à couper toute communication entre la borne et le central de surveillance en utilisant des dispositifs adaptés tels que des dispositifs de brouillage des signaux GSM.

**[0009]** Le but de l'invention est de remédier aux inconvénients de l'art antérieur en fournissant une solution de dissuasion contre les attaques de terminaux qui soit tout à la fois fiable et peu coûteuse.

**[0010]** Selon un premier objet de l'invention, celle-ci porte sur un procédé de surveillance d'une pluralité de terminaux, notamment d'horodateurs, dans lequel au moins des premier et second terminaux sont équipés de moyens de communication permettant aux dits premier et second terminaux de communiquer entre eux et avec un central de surveillance.

**[0011]** Selon une définition générale de l'invention, le procédé comprend un protocole de surveillance selon lequel les premier et second terminaux doivent s'appeler, de préférence mutuellement et à une cadence prédéterminée, et en cas d'absence d'appel et/ou de non-réponse de la part du second terminal, ledit premier terminal est apte à appeler le central de surveillance pour l'informer de la situation anormale concernant le second terminal.

**[0012]** La mise en oeuvre de ce procédé amène chacun des terminaux à surveiller ses voisins et à être lui-même surveillé par ses voisins.

**[0013]** Au niveau du parc de terminaux, une surveillance interne a donc lieu, sans l'intervention du central de

surveillance.

**[0014]** Cette surveillance a lieu à l'aide de communications inter-terminaux ne nécessitant pas de frais d'opérateur de télécommunication.

5 **[0015]** Une communication téléphonique vers le central de surveillance n'est déclenchée que lorsqu'une anomalie s'est effectivement produite, c'est-à-dire lorsque l'un des terminaux détecte l'absence de réponse de l'un de ses voisins ou bien lorsque l'un des terminaux détecte  
10 une tentative d'attaque à son encontre.

**[0016]** Selon un autre mode de réalisation, le protocole de surveillance comprend en outre une étape selon laquelle chacun des terminaux signale une éventuelle attaque frauduleuse à son encontre en contactant directement le central de surveillance ou en contactant un terminal voisin qui se chargera de contacter le central de surveillance.

15 **[0017]** D'autre part, les communications entre les terminaux peuvent être effectuées au moyen d'un réseau local radioélectrique.

20 **[0018]** De plus, les communications entre un terminal et le central de surveillance peuvent être effectuées au moyen d'un réseau téléphonique ouvert au public.

**[0019]** Selon un deuxième objet de l'invention, celle-ci vise un dispositif de surveillance d'une pluralité de terminaux, notamment d'horodateurs, du type comprenant au moins des premier et second terminaux voisins l'un de l'autre et équipés de moyens de communication permettant auxdits premier et second terminaux de communiquer entre eux et avec un central de surveillance, les premier et second terminaux devant s'appeler mutuellement à une cadence choisie et le dispositif comprenant des moyens de surveillance logés dans au moins le premier terminal et aptes en cas d'absence d'appel et/ou de non-réponse de la part du second terminal à appeler le central de surveillance pour l'informer de la situation anormale concernant le second terminal.

30 **[0020]** L'invention a également pour objet un terminal comportant des moyens de communication permettant de communiquer avec au moins un second terminal et avec un central de surveillance et des moyens de commande assurant l'émission d'appels à destination dudit second terminal et des moyens de surveillance aptes en cas d'absence d'appel et/ou de non-réponse de la part  
35 du second terminal à appeler le central de surveillance (4) pour l'informer de la situation anormale concernant le second terminal.

**[0021]** Selon un autre mode de réalisation, ledit terminal doit appeler au moins un terminal voisin à une cadence choisie

40 **[0022]** Selon un autre mode de réalisation particulier, le terminal comprend en outre des moyens de détection d'attaques frauduleuses et est apte à signaler une éventuelle attaque à son encontre en contactant directement le central de surveillance ou en contactant un terminal voisin qui se chargera de contacter le central de surveillance.

45 **[0023]** Les moyens permettant audit terminal de com-

muniquer avec les autres terminaux peuvent comprendre un dispositif radioélectrique émetteur-récepteur.

**[0024]** Les moyens permettant audit terminal de communiquer avec le central de surveillance peuvent comprendre des moyens de raccordement à un réseau téléphonique ouvert au public.

**[0025]** D'autres caractéristiques et avantages de l'invention apparaîtront à la lumière de la description donnée ci-après et des dessins dans lesquels :

- la figure 1 représente une paire d'horodateurs et un central de surveillance, un premier horodateur recevant un appel d'un second horodateur ;
- la figure 2 représente une paire d'horodateurs et un central de surveillance, un premier horodateur effectuant un appel vers un second horodateur.

**[0026]** L'ensemble représenté sur les figures 1 et 2 est composé d'un parc d'horodateurs réduit au minimum pour des raisons de clarté (deux horodateurs 1, 2 seulement), d'un réseau téléphonique 3 et d'un central de surveillance schématisé par un micro-ordinateur 4.

**[0027]** Dans l'exemple décrit, le réseau téléphonique 3 est un réseau sans-fil tel que le réseau européen GSM mais peut être un quelconque réseau de communication, par exemple ouvert au public tel que le réseau filaire RTC et analogues.

**[0028]** Le central de surveillance 4 dispose de moyens de traitement informatique reliés au réseau téléphonique 3 et aptes à recevoir et traiter des appels provenant d'un horodateur 1 ; 2.

**[0029]** Les horodateurs 1, 2 composant le parc sont équipés de moyens informatiques de traitement de l'information et sont également équipés de moyens de liaison au réseau téléphonique 3 aptes à appeler le central de surveillance 4 et à lui transmettre un signal d'alerte.

**[0030]** Le signal d'alerte se présente comme un code binaire élaboré par l'équipement informatique d'un horodateur 1 ; 2 et transmis sous forme modulée via le réseau téléphonique 3 vers le central de surveillance 4.

**[0031]** Lors de la réception du signal d'alerte, le central de surveillance 4 démodule le signal reçu pour obtenir le code binaire initial et l'identifie comme étant un signal d'alerte.

**[0032]** Il est nécessaire à cet effet d'établir préalablement un protocole de communication entre le central téléphonique 4 et les horodateurs 1, 2 pour définir le code binaire correspondant à un signal d'alerte.

**[0033]** De la même manière, d'autres codes correspondant à d'autres informations qui pourraient être transmises entre le central de surveillance 4 et les horodateurs 1, 2 peuvent être définis.

**[0034]** Les horodateurs 1, 2 sont d'autre part équipés de moyens de transmission radioélectriques rendant chaque horodateur apte à communiquer avec tous les horodateurs se trouvant dans la zone de couverture de ses moyens de transmission.

**[0035]** Par exemple, les moyens de transmission sont constitués par des cartes réseau répondant aux normes de transmission sans-fil IEEE 802.11b permettant aux horodateurs de communiquer entre eux en employant le protocole TCP/IP, un tel protocole n'est donné qu'à titre illustratif et n'est pas limitatif de la présente invention. La communication entre les horodateurs s'effectuent de préférence en utilisant un réseau de type WLL (wireless local loop) c'est-à-dire un réseau radioélectrique sans fil. Différentes gammes de fréquences sont utilisables et notamment les fréquences infrarouges, protocole Blue Tooth par exemple. L'intérêt d'un tel mode de communication est qu'il est gratuit.

**[0036]** L'ensemble qui vient d'être décrit fonctionne de la manière indiquée ci-après.

**[0037]** Le parc d'horodateurs 1, 2 est installé dans les rues d'une ville de manière que chacun se trouve dans la zone de couverture des moyens de transmission électromagnétiques d'au moins un autre horodateur.

**[0038]** En fonctionnement normal, chaque horodateur contacte au moins son voisin le plus proche dont les coordonnées lui ont été préalablement communiquées pour vérifier qu'il fonctionne bien et est, par conséquent, lui-même contacté par ses voisins.

**[0039]** De même que pour la communication avec le central de surveillance 4, il est nécessaire de définir un protocole par lequel les horodateurs vérifieront mutuellement leur bon fonctionnement.

**[0040]** A ces fins, un code d'appel et un code de confirmation sont définis. Lorsqu'il contacte l'un de ses voisins, chaque horodateur envoie le code d'appel et attend le code de confirmation pour considérer que l'horodateur contacté fonctionne correctement.

**[0041]** Par conséquent, chaque horodateur doit également envoyer le code de confirmation à chacun des horodateurs le sollicitant par l'envoi du code d'appel.

**[0042]** Par ailleurs et pour limiter la consommation d'énergie, seuls les moyens de transmission radioélectriques sont alimentés pendant les périodes de veille, assurant ainsi les fonctions de vérifications mutuelles des terminaux sans dépenses d'énergie qui ne soit pas absolument nécessaire.

**[0043]** La figure 1 représente un horodateur 2 effectuant un envoi du code d'appel vers un horodateur 1 voisin et la figure 2 représente une situation similaire, l'horodateur 1 envoyant cette fois-ci le code de confirmation en réponse à l'horodateur 2.

**[0044]** Dans le cas où l'horodateur 2 est défaillant, l'envoi du code d'appel illustré à la figure 1 ne se produit pas et l'horodateur 1, qui attend périodiquement le code d'appel de la part de l'horodateur 2, détecte le silence de cet horodateur 2 et interprète cela comme une défaillance de l'horodateur 2.

**[0045]** L'horodateur 1 téléphone alors au central de surveillance 4 et lui transmet le code d'alerte en identifiant l'horodateur 2 resté muet.

**[0046]** De même, dans le cas où l'horodateur 1 est cette fois-ci défaillant, l'envoi du code de confirmation

illustré à la figure 2 ne se produit pas et l'horodateur 2, qui attend le code de confirmation de la part de l'horodateur 1, détecte le silence de cet horodateur 1 et interprète cela comme une défaillance de l'horodateur 1.

[0047] L'horodateur 2 téléphone alors au central de surveillance 4 et lui transmet le code d'alerte en identifiant l'horodateur 1 resté muet.

[0048] D'autre part, chaque horodateur est également équipé de moyens de détection d'attaques aptes à détecter des attaques physiques tel qu'un ensemble de capteurs disposés sur les composants de l'horodateur et aptes également à détecter des attaques sur ses voies de communications tels que des dispositifs de sécurité informatique rendant compte d'une tentative de brouillage électromagnétique ou de connexion frauduleuse à l'équipement informatique de l'horodateur.

[0049] Dans le cas où un horodateur détecte une telle attaque sur lui-même, cet horodateur a la possibilité d'une part d'appeler lui-même le central de surveillance 4 pour se déclarer victime d'une attaque ou bien, d'autre part de transmettre un signal d'alerte à l'un de ses voisins qui contactera le central de surveillance.

[0050] Ces possibilités peuvent être utilisées en combinaison pour un maximum de sécurité, le central de surveillance 4 étant alerté même si l'un des deux moyens de communication de l'horodateur attaqué est mis hors service par l'attaque.

[0051] L'invention mise en oeuvre permet d'obtenir les avantages suivants :

- une réduction des coûts de fonctionnement d'un parc d'horodateurs par la limitation au strict nécessaire des appels payants vers le central de surveillance et l'utilisation alternative des communications inter-terminaux, celles-ci étant sans frais dans la mesure où elles ne font pas intervenir d'opérateur téléphonique ;
- les attaques ciblées sur les moyens de communications des horodateurs sont également détectées ;
- les dépenses en énergie des terminaux sont minimisées par l'alimentation sélective des composants autorisant la mise en service uniquement des moyens de transmission inter-terminaux pendant les périodes de veille ;
- une réactivité quasi-immédiate aux attaques, chaque terminal pouvant lui-même signaler une attaque à son encontre.

## Revendications

1. Procédé de surveillance d'une pluralité de terminaux automatiques de paiement (1, 2), tels que des horodateurs, dans lequel au moins des premier (1) et second (2) terminaux sont équipés de moyens de communication permettant aux dits premier et second terminaux (1, 2) de communiquer entre eux et avec un central de surveillance (4), le procédé com-

prenant un protocole de surveillance selon lequel les premier et second terminaux (1, 2) doivent s'appeler, et en cas d'absence d'appel et/ou de non-réponse de la part du second terminal (2), ledit premier terminal (1) est apte à appeler le central de surveillance (4) pour l'informer d'une situation anormale concernant le second terminal (2).

2. Procédé de surveillance selon la revendication 1, **caractérisé en ce que** selon ledit protocole de surveillance lesdits premier et second terminaux doivent s'appeler mutuellement à une cadence prédéterminée.
3. Procédé de surveillance selon l'une quelconque des revendications précédentes, **caractérisé en ce que** le protocole de surveillance comprend en outre une étape selon laquelle chacun des terminaux (1, 2) signale une éventuelle attaque frauduleuse à son encontre en contactant directement le central de surveillance (4) ou en contactant un terminal voisin qui se chargera de contacter le central de surveillance (4).
4. Procédé de surveillance selon l'une quelconque des revendications précédentes, **caractérisé en ce que** chaque terminal appelle selon ledit protocole de surveillance plusieurs terminaux distincts.
5. Procédé de surveillance selon l'une quelconque des revendications précédentes, **caractérisé en ce que** les communications entre les terminaux (1, 2) sont effectuées au moyen d'un réseau local radioélectrique.
6. Procédé de surveillance selon l'une quelconque des revendications précédentes, **caractérisé en ce que** les communications entre un terminal (1 ; 2) et le central de surveillance (4) sont effectuées au moyen d'un réseau téléphonique ouvert au public.
7. Procédé de surveillance selon l'une quelconque des revendications précédentes, **caractérisé en ce que** lesdits premier et second terminaux sont voisins l'un de l'autre.
8. Dispositif de surveillance d'une pluralité de terminaux, notamment d'horodateurs, du type comprenant au moins des premier (1) et second (2) terminaux et équipés de moyens de communication permettant auxdits premier et second terminaux de communiquer entre eux et avec un central de surveillance (4), dans lequel les premier et second terminaux (1, 2) doivent s'appeler et dans lequel des moyens de surveillance logés dans au moins le premier terminal (1) sont aptes en cas d'absence d'appel et/ou de non-réponse de la part du second terminal (2) à appeler le central de surveillance (4) pour

l'informer d'une situation anormale concernant le second terminal (2).

9. Terminal automatique de paiement tel qu'un horodateur (1) comportant des moyens de communication permettant de communiquer avec au moins un second terminal (2) et avec un central de surveillance (4) et des moyens de commande assurant l'émission d'appels à destination dudit second terminal (2) et des moyens de surveillance aptes en cas d'absence d'appel et/ou de non-réponse de la part du second terminal (2) à appeler le central de surveillance (4) pour l'informer de la situation anormale concernant le second terminal (2).
10. Terminal selon la revendication 9, **caractérisé en ce que** ledit terminal doit appeler au moins ledit second terminal selon une cadence choisie.
11. Terminal selon la revendication 9 ou 10, **caractérisé en ce qu'il** comprend en outre des moyens de détection d'attaques frauduleuses et est apte à signaler une éventuelle attaque à son encontre en contactant directement le central de surveillance (4) ou en contactant un terminal voisin qui se chargera de contacter le central de surveillance (4).
12. Terminal selon l'une des revendications 9 à 11, **caractérisé en ce que** les moyens permettant audit terminal de communiquer avec ledit second terminal comprennent un dispositif radioélectrique émetteur-récepteur.
13. Terminal selon l'une des revendications 9 à 11, **caractérisé en ce que** les moyens permettant audit terminal de communiquer avec le central de surveillance (4) comprennent des moyens de raccordement à un réseau téléphonique ouvert au public.

## Claims

1. Method of monitoring a plurality of automatic terminals (1, 2) for making payment, such as date and time machines, wherein at least first (1) and second (2) terminals are provided with communication means allowing said first and second terminals (1, 2) to communicate with one another and with a monitoring centre (4), the method including a monitoring protocol according to which the first and second terminals (1, 2) must call one another and, in the event of absence of a call from and/or non-response by the second terminal (2), said first terminal (1) is arranged to call the monitoring centre (4) to inform it of an abnormal situation concerning the second terminal (2).
2. Monitoring method according to claim 1, **character-**

**ised in that** according to said monitoring protocol said first and second terminals must mutually call one another with predetermined timing.

3. Monitoring method according to any one of the preceding claims, **characterised in that** the monitoring protocol additionally includes a step according to which each of the terminals (1, 2) signals a possible fraudulent attack against it by directly contacting the monitoring centre (4) or by contacting a neighbouring terminal, which will assume the task of contacting the monitoring centre (4).
4. Monitoring method according to any one of the preceding claims, **characterised in that** according to said monitoring protocol each terminal calls a plurality of different terminals.
5. Monitoring method according to any one of the preceding claims, **characterised in that** the communications between the terminals (1, 2) are carried out by means of a radio local network.
6. Monitoring method according to any one of the preceding claims, **characterised in that** the communications between a terminal (1; 2) and the monitoring centre (4) are carried out by means of a telephone network accessible to the public.
7. Monitoring method according to any one of the preceding claims, **characterised in that** said first and second terminals neighbour one another.
8. Arrangement for monitoring a plurality of terminals, especially date and time machines, of the type comprising at least first (1) and second (2) terminals and provided with communication means allowing said first and second terminals to communicate with one another and with a monitoring centre (4), wherein the first and second terminals (1, 2) must call one another and wherein monitoring means accommodated in at least the first terminal (1) are, in the event of absence of a call from and/or non-response by the second terminal (2), arranged to call the monitoring centre (4) to inform it of an abnormal situation concerning the second terminal (2).
9. Automatic terminal for making payment, such as a date and time machine (1), comprising communication means allowing it to communicate with at least one second terminal (2) and with a monitoring centre (4) and control means which provide for the transmission of calls destined for said second terminal (2) and monitoring means which, in the event of absence of a call from and/or non-response by the second terminal (2), are arranged to call the monitoring centre (4) to inform it of the abnormal situation concerning the second terminal (2).

10. Terminal according to claim 9, **characterised in that** said terminal must call at least said second terminal in accordance with selected timing.
11. Terminal according to claim 9 or 10, **characterised in that** it additionally comprises means for detecting fraudulent attacks and it is arranged to signal a possible attack against it by directly contacting the monitoring centre (4) or by contacting a neighbouring terminal, which will assume the task of contacting the monitoring centre (4).
12. Terminal according to one of claims 9 to 11, **characterised in that** the means allowing said terminal to communicate with said second terminal comprise a radio transmitter-receiver device.
13. Terminal according to one of claims 9 to 11, **characterised in that** the means allowing said terminal to communicate with the monitoring centre (4) comprise means for connecting to a telephone network accessible to the public.

#### Patentansprüche

1. Verfahren zur Überwachung einer Vielzahl von automatischen Zahlterminals (1, 2), wie Zeitstempel, bei welchem zumindest ein erster (1) und zweiter (2) Terminal mit Kommunikationsvorrichtungen ausgestattet sind, welche dem ersten und zweiten Terminal (1, 2) erlauben, miteinander und mit einer Überwachungszentrale (4) zu kommunizieren, wobei das Verfahren ein Überwachungsprotokoll umfasst, gemäß welchem sich der erste und zweite Terminal (1, 2) gegenseitig anrufen müssen und im Falle des Fehlens eines Anrufs und/oder des Nicht-Antwortens des zweiten Terminals (2), der erste Terminal (1) in der Lage ist, die Überwachungszentrale (4) anzurufen, um sie über die anormale Situation des zweiten Terminals (2) zu informieren.
2. Überwachungsverfahren gemäß Anspruch 1, **dadurch gekennzeichnet, dass** sich der erste und zweite Terminal gemäß diesem Überwachungsprotokoll gegenseitig in einer vorbestimmten zeitlichen Abfolge anrufen müssen.
3. Überwachungsverfahren gemäß irgendeinem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass** das Überwachungsprotokoll außerdem einen Schritt umfasst, gemäß welchem jeder der Terminals (1, 2) einen eventuellen betrügerischen Angriff gegen ihn selbst anzeigt, indem er die Überwachungszentrale (4) direkt kontaktiert oder indem er einen Nachbarterminal kontaktiert, der sich zur Aufgabe macht, die Überwachungszentrale (4) zu kontaktieren.

4. Überwachungsverfahren gemäß irgendeinem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass** jeder Terminal gemäß diesem Überwachungsprotokoll mehrere verschiedene Terminals anruft.
5. Überwachungsverfahren gemäß irgendeinem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass** die Kommunikationen zwischen den Terminals (1, 2) mit Hilfe eines lokalen radioelektrischen Netzes durchgeführt werden.
6. Überwachungsverfahren gemäß irgendeinem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass** die Kommunikationen zwischen einem Terminal (1; 2) und der Überwachungszentrale (4) mit Hilfe eines der Öffentlichkeit zugänglichen Telefonnetzes hergestellt werden.
7. Überwachungsverfahren gemäß irgendeinem der vorherigen Ansprüche, **dadurch gekennzeichnet, dass** der erste und zweite Terminal zueinander benachbart sind.
8. Vorrichtung zur Überwachung einer Vielzahl von Terminals, insbesondere von Zeitstempeln, der Art mit zumindest einem ersten (1) und zweiten (2) Terminal, die mit Kommunikationsvorrichtungen ausgestattet sind, welche dem ersten und zweiten Terminal ermöglichen miteinander und mit einer Überwachungszentrale (4) zu kommunizieren, wobei der erste und zweite Terminal (1, 2) sich gegenseitig anrufen müssen, und wobei Überwachungseinrichtungen, die in zumindest dem ersten Terminal (1) gelagert sind, dazu in der Lage sind, im Fall des Fehlens eines Anrufs und/oder des Nicht-Antwortens seitens des zweiten Terminals (2), die Überwachungszentrale (4) anzurufen, um sie über die anormale Situation bezüglich des zweiten Terminals (2) zu informieren.
9. Automatischer Zahlterminal, wie ein Zeitstempel (1), mit Kommunikationsvorrichtungen, welche ermöglichen mit zumindest einem zweiten Terminal (2) und mit einer Überwachungszentrale (4) zu kommunizieren, und Steuervorrichtungen, welche die Ausgabe von Anrufen in Richtung des zweiten Terminals (2) sicherstellen, und Überwachungsvorrichtungen, die in der Lage sind, im Fall des Fehlens eines Anrufs und/oder des Nicht-Antwortens seitens des zweiten Terminals (2) die Überwachungszentrale (4) anzurufen, um sie über die anormale Situation bezüglich des zweiten Terminals (2) zu informieren.
10. Terminal gemäß Anspruch 9, **dadurch gekennzeichnet, dass** der Terminal zumindest den zweiten Terminal gemäß einer gewählten zeitlichen Abfolge anrufen muss.

11. Terminal gemäß Anspruch 9 oder 10, **dadurch gekennzeichnet, dass** er außerdem Vorrichtungen zur Erfassung betrügerischer Angriffe aufweist, und er in der Lage ist, einen eventuellen Angriff gegen ihn anzuzeigen, indem er die Überwachungszentrale (4) direkt kontaktiert oder indem er einen Nachbarterminal kontaktiert, der sich zur Aufgabe macht, die Überwachungszentrale (4) zu kontaktieren. 5
12. Terminal gemäß einem der Ansprüche 9 bis 11, **dadurch gekennzeichnet, dass** die Vorrichtungen, welche dem Terminal ermöglichen, mit den zweiten Terminal zu kommunizieren, eine radioelektrische Sende-Empfangs-Vorrichtung aufweisen können. 10 15
13. Terminal gemäß einem der Ansprüche 9 bis 11, **dadurch gekennzeichnet, dass** die Vorrichtungen, welche dem Terminal ermöglichen, mit der Überwachungszentrale (4) zu kommunizieren, Einrichtungen zum Anschluss an ein der Öffentlichkeit zugängliches Telefonnetz aufweisen können. 20 25 30 35 40 45 50 55

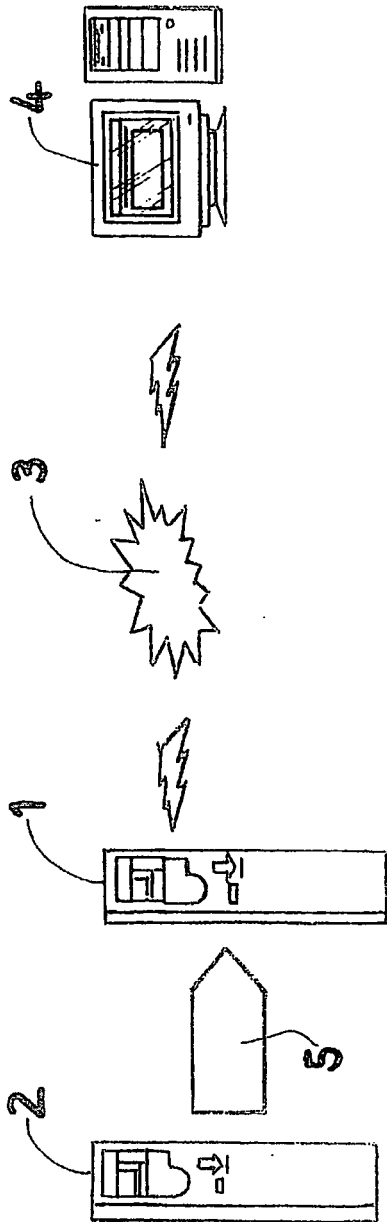


**FIG. 1**

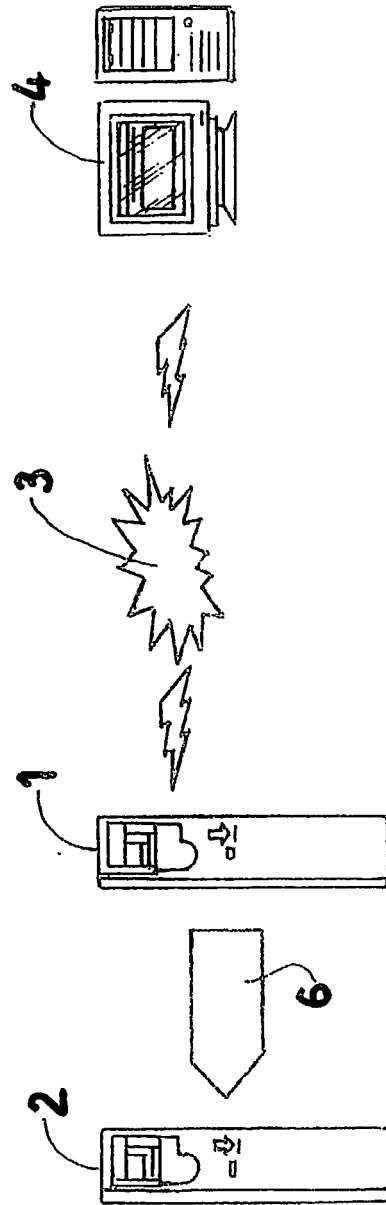


**FIG. 2**