(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 243 192 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
01.07.2020 Bulletin 2020/27

(21) Application number: **16735295.4**

(22) Date of filing: **05.01.2016**

(51) Int Cl.:
G08B 17/12 *(2006.01)* ***G06F 15/16*** *(2006.01)*
G08B 25/00 *(2006.01)* ***G08B 21/12*** *(2006.01)*
G08B 26/00 *(2006.01)*

(86) International application number:
PCT/US2016/012174

(87) International publication number:
WO 2016/112006 (14.07.2016 Gazette 2016/28)

(54) **INTELLIGENT SERVER IN A SYSTEM OF NETWORKED SENSORS**

INTELLIGENTER SERVER IN EINEM SYSTEM AUS VERNETZTEN SENSOREN

SERVEUR INTELLIGENT DANS UN SYSTÈME DE CAPTEURS EN RÉSEAU

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **07.01.2015 US 201562100700 P**

(43) Date of publication of application:
15.11.2017 Bulletin 2017/46

(73) Proprietor: **Passport Systems, Inc.**
Billerica, MA 01862 (US)

(72) Inventors:
- **COOPER, Daniel, A.**
  Billerica, MA 01862 (US)
- **COSTALES, James, B.**
  Billerica, MA 01862 (US)
- **KAMIENIECKI, Krzysztof, E.**
  Billerica, MA 01862 (US)
- **LEDOUX, Robert, J.**
  Billerica, MA 01862 (US)
- **THOMPSON, Jeffrey, K.**
  Billerica, MA 01862 (US)
- **KORBLY, Stephen, E.**
  Billerica, MA 01862 (US)

(74) Representative: **Hibbert, Juliet Jane Grace et al**
Kilburn & Strode LLP
Lacon London
84 Theobalds Road
London WC1X 8NL (GB)

(56) References cited:
WO-A2-2004/051868 **WO-A2-2004/051868**
CN-A- 103 546 966 **US-A1- 2014 099 882**
US-A1- 2014 099 882

- **KOUTSOUKOS XENOFON ET AL: "OASiS: A Service-Oriented Architecture for Ambient-Aware Sensor Networks", 16 October 2006 (2006-10-16), MEDICAL IMAGE COMPUTING AND COMPUTER-ASSISTED INTERVENTION - MICCAI 2015 : 18TH INTERNATIONAL CONFERENCE, MUNICH, GERMANY, OCTOBER 5-9, 2015; PROCEEDINGS; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER INTERNATIONAL PUBLISHING, CH, XP047302805, ISSN: 0302-9743 ISBN: 978-3-540-70543-7 * figures 2,6 * * page 1, paragraph 1 * * page 5, paragraph 2.2 * * page 17, paragraph 3 ***

EP 3 243 192 B1

Description

BACKGROUND

[0001] There is a growing concern that a radiological dispersal device ("dirty bomb") could be used by terrorist particularly in places with a high density of people or in areas of high value commercial or government properties and facilities. Since such a device would be small enough to be man or vehicle portable, the best probability to detect and interdict such a device is to widely distribute a network of spectroscopic radiation sensors that are mobile, man portable, work without operator intervention and are connected to central command and control sensor and optionally to one another. This provides the most general and dynamic scheme to monitor and map a large, uncontrolled area potentially full of people. An additional important benefit of such a system is that it can detect radioactive sources that, although not intended as terrorist threats, still pose public safety problems. For example, there have been incidents where untended industrial and medical sources have been released without proper safeguards into public areas.

[0002] Any local measurement of radiation has contributions from Naturally Occurring Radioactive Materials (NORM) in that locale and possible non-NORM sources ranging from medical isotopes (from patients for example which just underwent a stress test), industrial isotopes not properly secured or being used for nefarious purposes and Special Nuclear Materials (SNM) that can be used in a nuclear device (or a nuclear device already assembled). Detection algorithms must estimate the contributions of both NORM backgrounds and the presence of possible non-NORM radioactive sources.

[0003] The detection of natural and manmade sources using distributed radiation sensors over large geographic areas poses unique and complex networking and computational problems. It has been demonstrated that fusing spectral data from sensors that are in proximity offers higher sensitivity and low false alarm rates, for example, as described in PCT/US2014/012330, published as WO 2014/0133687, and U.S. Pat. App. US2017/0003404. The spatial scale over which spectral data fusion is useful is determined by intrinsic sensor properties such as the absolute efficiency, and energy resolution of the sensor. External properties of importance are the energy, and strength of the radioactive source and any shielding materials that are between the source and sensor. For example, spatial scales of order few times 10 m are obtained for handheld spectroscopic radiation sensors. Thus in a large system of tens of thousands of sensors in a city there may be a large number of clusters of sensors in which real time sharing (of order seconds) of spectral data through a server or system of servers is helpful to reap the full benefits of spectral data fusion. Efficient and responsive network systems can generate a dynamic set of clusters that allow full data sharing for optimal detection performance. For sensor nodes that are isolated (i.e., nodes that do not benefit from real time data sharing), data transmission will consist of node position, health, background spectra measurements and any detection alarms. The network SmartServer can dynamically determine if open bandwidth is present so that even isolated nodes can dynamically transmit spectral data for background mapping. Optionally, if the Server determines that open bandwidth is not present the node can locally log data and upload to the system when bandwidth is available and/or there is a local "base" connection to the server. It is also desirable for two way communication between command and control provided through the SmartServer. Usually the required bandwidth for such communication consists of passing alarms, texts, etc. and is typically small as compared to that required for data fusion.

[0004] As discussed above, a high spatial resolution statistically significant map of the NORM background is crucial for high sensitivity searches for non-NORM radiation sources. NORM background can vary significantly over small spatial scales particularly in urban environmental with a large variety of construction materials are present. Therefore, fine scale measurements of the background are highly desirable to ensure high sensitivity to the presence of non-NORM sources of radiation while retaining a low rate of false alarms. A distributed network of radiation sensors with spectroscopic capabilities is an effective method for obtaining large area coverage of NORM background. Particularly if the sensors are mobile, they can differentiate isotopes of interest and can do this without operator intervention or supervision. Therefore, optimal network architecture must be able to collect, store and distribute this constantly updated background map. In a large system, a SmartServer can improve performance by allocating the available resources between the search for non-NORM sources of radiation and the collection and distribution of background data.

[0005] Reference is made to the following article by Koutsoukos Xenofon et al, "OASiS: A Service-Oriented Architecture for Ambient-Aware Sensor Networks", from Medical Image Computing and Computer-Assisted Intervention - MICCAI 2015 : 18th International Conference, Munich, Germany, October 5-9, 2015, which describes OASiS, a lightweight service-oriented architecture for sensor networks, which provides dynamic service discovery and can be used to develop ambient-aware applications.

[0006] Chinese patent application CN103546966 relates to a node positioning method of a wireless sensor based on a field environment. The node positioning method comprises sensing the neighborhood relationship among the nodes to obtain an index for measuring the distance, the neighborhood relationship comprises the number of the neighborhood nodes of each node and the absolute distance relationship between the nodes and the index is the common neighborhood distance; the estimation position of the unknown node is determined according to the index; the position of the unknown node

is corrected according to the neighborhood relationship and the estimation position.

[0007] PCT patent application no. WO2004051868 describes a system to detect, classify, and locate sources of RF activity. The system comprises one or more sensors positioned at various locations in a region where activity in a shared radio frequency band is occurring and a server coupled to the sensors. Each sensor monitors communication traffic, such as IEEE WLAN traffic, as well as classifies non-WLAN signals occurring in the frequency band. The server receives data from each of the plurality of sensors and executes functions to process the data supplied by the plurality of sensors.

[0008] US patent application US2014099882 describes a communication system comprising one or more self-powered satellite units each providing signal information to at least one command console through a segmented cable assembly system in operable communication with a central station that receives signal information from the at least one command console and relays signal information back to the command console wirelessly and via the segmented cable assembly system.

SUMMARY

[0009] A large system of networked sensors requires the management and distribution of sensor data via an intelligent server (SmartServer). In this network of sensors, one or more SmartServers use the underlying processes of source detection to optimize network data flow.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010]

FIG. 1 schematically shows one possible arrangement of elements in a system with dynamic node grouping.

FIG. 2 shows schematically a series of sensor nodes spread out around an intersection of streets.

FIG. 3 shows the same set of sensor nodes as FIG. 2, now divided into four groups, shown schematically with dashed lines.

FIG. 4 shows the same set of sensor nodes as FIGS. 2 and 3 in their groups, but now adds a source moving along one of the streets toward the intersection.

DETAILED DESCRIPTION

[0011] The invention is defined by the appended claims. The presence of a source can be detected using a network of sensors. The network of sensors includes mobile and fixed sensors. In order to patrol an area, mobile sensors are carried by a group of people walking or mounted on vehicles. Mobile sensors are connected to a network through a wired or wireless connection. The people that would patrol an area using mobile sensors include, but not limited to, security personnel and first responders. Fixed sensors are situated in a permanent location, where constant monitoring is preferred or required. Locations that would use a fixed sensor include, but are not limited to, security checkpoints, major intersections, exits or entrances of buildings, or other significant, high importance locations. Fixed sensors are connected to a network through a wired or wireless connection. The detector may be a radiation detector, a chemical detector, or any other suitable detector for the source in question. In normal operation each networked sensor collects data that may be transmitted to a central node (for processing and archiving) or other mobile sensor nodes in the network, and the sensor nodes may in turn receive such signals, either from other sensor nodes or from a central node, with the result that data from the network as a whole is collectively processed to determine if, when, and where a source is present.

[0012] As explained in WO 2014/0133687, sources can be detected in real time by analysis of data collected by a network of sensors. Computation and detection can be carried out in a single central computer, or on a plurality of distributed computers, for example, in processors located at each sensor node in the network. Computational detection can be carried out on a data set obtained from any collection of sensors, for example, all sensors in the network, or one or more subsets of all sensors in the network. Carrying out the computational detection algorithms using data obtained from only a subset of the sensors can have several advantages, as explained below, depending on how the subset is defined.

[0013] FIG. 1 schematically shows one possible arrangement of elements in a system with dynamic node grouping. Data is stored in a database 1. Servers 2, 3, 4, communicate with the database 1. Each server is associated with a group 5, 6, 7 of nodes, e.g., 5a-5d, etc., in the network. The nodes are dynamically grouped according to the conditions of the system. As shown, each server has an equal number of nodes, but this need not be true generally; because the node grouping is dynamically responsive to system conditions, the number of nodes in each grouping will vary from group to group and over time. In this case, the nodes 5a-5d each carries a sensor for detecting a material of interest, e.g., a radiation or chemical sensor, and may also include elements capable of determining the sensor's position, velocity, orientation and acceleration. Each sensor node 5a-5d in the group 5 communicates with its designated server 2. The server 2 can carry out multiple functions. The server 2 can operate on the data reported from the nodes 5a-5d to determine whether a source has been detected, for example, by using the methods described in WO 2014/0133687. Alternatively, the detection process can be carried out on other computers, such as central processing node, or alternatively on computers on board each sensor node, while the servers 2, 3, 4 focus on the optimal assignment of nodes to groups. The server 2 can communicate with the other servers 3, 4 to determine whether any of the sensor nodes 5a-5d should be moved

to another node group 6, 7. For example, the server 2 can compare the locations of the various nodes to determine whether one node has moved from a geographic area associated with a first group into a geographic area associated with a second group. A server can communicate with other servers to determine whether a source has been detected in a node group, in which case the server might move nodes into or out of the group in which a detection has been made. A server might measure the amount of network traffic amongst the nodes in its group and, by comparing to the traffic in other groups, determine that system performance could be improved or optimized if a node were to be moved from one group to another.

[0014] As shown in FIG. 1, all the servers can be physically distinct, networked computers with their own dedicated processors. Alternatively, a system capable of all the same functionality could be set up with a single server assigning nodes into subgroups. In that case, a single server would collect the necessary data from all nodes on the network, analyze the relevant network and system parameters such as network traffic, geography, and presence or absence of detections, and determine whether the current grouping or an alternative grouping is preferred.

[0015] Node groupings can be optimized to various effects. For example, in a system where each node communicates with every other node in the group, the quantity of network traffic in a single group will be of order of the square of the number of nodes in the group. By dividing the nodes into N groups, the total traffic on the system will be reduced by roughly a factor of N compared to the case where all nodes are in a single system-wide group. Node groupings can also be based simply on geography. Each sensor node will have a certain sensitivity, and correspondingly a certain geographic range over which it is likely to be sensitive to the presence of a source. Sensor nodes may be grouped to make sure that the ranges of the nodes in a given group overlap sufficiently to provide full coverage of a certain geographic area. This may change over time, as sensor nodes may be moved, as with nodes that are attached to patrol personnel.

[0016] It may also be advantageous to group nodes geographically once a source has been detected. For example, if a moving source has been detected, the system could dynamically group nodes so as to follow the motion of the source, always having a higher concentration of nodes near where the source is expected to be based on its last estimated velocity. Similarly, in the case of a tentative detection, the system may allocate more nodes to a group near the tentative detection to follow-up.

[0017] The system may also expand the geographical size of a group in response to a detection or tentative detection. For example, if each group is initially designated to cover an predetermined area, say 10,000 square meters, and a detection or tentative detection is made in one such grouping, it may be helpful to merge adjacent groups into the group where a detection was made in order to pursue that source and increase confidence that the source will not move undetected out of its current group.

[0018] Similarly, the system may take into account *a priori* knowledge of the geography to group nodes intelligently. For example, the system may group nodes, not simply by geographic proximity to each other, but rather by proximity to existing landmarks, such as streets. Rather than a grouping defined by a single radius, the system could group nodes along a single street, or around an intersection. See discussion of FIGS. 2-4 below.

[0019] Grouping sensor nodes is also an indirect way of intelligently allocating computing power. In any detection algorithm, such as the particle filtering algorithm described in WO 2014/0133687, analysis of more data requires more computing power. But more data does not necessarily increase useful sensitivity of the detection algorithm. For example, if two groups of sensors are geographically segregated to the point where their ranges do not significantly overlap, it may be more computationally efficient to treat the two groups totally separately. Data from the first group will not typically help the system detect a source in the geographic area of the second group, and vice versa. So there is no benefit to including all the data in a single detection calculation, only computational cost. Particle filtering algorithms are particularly well-suited to use with this sort of dynamic grouping. Each particle represents a possible state in phase space including information like source location, velocity and strength, and potentially sensor properties as well. Since every group in which a particle filtering algorithm is being run will use the same type of particles, those particles can easily be passed from one group to another. This can be useful, for example, in tracing the movement of a source from one geographic area to another.

[0020] Typically the initial assignment of sensor nodes to groups will be based on *a priori* knowledge of the geographic area in which the system is operating. Groups may be centered on a fixed position of interest, for example a secured entrance/exit from a building. The fixed position may be focused on one or more stationary sensor nodes. A group may be limited to sensors carried by personnel that are all part of a single unit, for example a particular group or squad of first responders, or a security team.

[0021] Another advantage of the present systems and methods is scalability. Unlike a networked system of nodes with full bi-directional communication between all nodes, in which the volume of communication traffic (as well as corresponding computational problems) is of order N^2, dividing the nodes up into groups allows an operator of the system to increase system traffic and computation roughly proportional to the number of nodes. An operator that wants to add another group of nodes to cover an additional geographic area need only add the additional number of nodes and a proportional increase in number or power of underlying servers. There is no need to scale the resources as N^2.

[0022] FIG. 2 shows schematically a series of sensor

nodes **11-25** spread out around an intersection of streets. A stationary node **11** is centered on the intersection, for example, a sensor installed on a traffic light. The other nodes **12-25** are schematically shown as smaller circles to indicate that they are mobile nodes, perhaps attached to a person or to a vehicle. FIG. 3 shows the same set of nodes divided into four groups, **26-29,** shown schematically with dashed lines. Each group covers a single street leading upto the intersection, but all groups include the stationary node **11** at the intersection. In this particular case, the groupings are defined by geography, but not simply by the range of the detectors. Such *a priori* knowledge of geography can be input into the system in the form of a map or series of maps and combined with location information from the various sensor nodes, for example, GPS data.

[0023] FIG. 4 shows the same sensor nodes in their groups, but now adds a source **30** that is detected, either confidently or tentatively, in group **28,** the source moving along one of the streets toward the intersection. In such a case, the system could make an algorithmic determination to expand group **28** to include, for example, nodes **18, 23,** and **12,** thereby allowing group **28** to continue accurately tracking the source **30** into and perhaps through the intersection. Or the system could combine all four groups **26-29** into a single group temporarily in order to determine which street the source **30** follows out of the intersection. Once the source **30** has left the intersection, where the node groups have a natural geographic overlap, the system could divide the nodes back out into their original groupings as the system continues to detect the source **30** moving along one of the streets.

[0024] In a situation such as the one described in FIG. 4, the system can also send feedback and instructions to the individual sensor nodes. For example, if the source is stopped in a particular location near the intersection, the system can instruct those carrying particular nodes to gather around the source to improve detection confidence, or to spread out in order to better capture future movements of the source.

[0025] In all the cases discussed herein, nodes can be grouped according to algorithms, based on *a priori* knowledge of the environment, based on specific instructions from human operators perhaps intervening in algorithmic decision-making, and any combinations thereof.

[0026] Methods of detecting a source can employ a plurality of nodes, each node including a sensor capable of collecting data and a transmitter configured to transmit at least sensor data collected by the sensor and location data representing at least the location of the node, a network capable of allowing transmission of data between and among the plurality of nodes and between the plurality of nodes and at least one computer, and a first computer having an input configured to receive data transmitted by nodes through the network, a memory configured to collect data transmitted by the nodes through the network, a processor configured to combine sensor and location data and compare the combined data to a predetermined detection criterion to determine whether a source is detected, and an output. Such methods can include collecting, in the first computer, location data transmitted through the network from each node to the first computer, the data being associated with a predetermined time, for each node, associating the node at the predetermined time with at least one of a plurality of node groups based at least in part on at least one of (a) a position of the node, (b) a velocity of the node, and (c) a measure of traffic on the network, for each node group, determining whether a source has been detected by the node group by combining, in the first computer, sensor data and location data collected from the nodes in the group and comparing, in the first computer, the combined sensor data and location data to at least one predetermined detection criterion, and signaling, with the output, at least whether a source has been detected.

[0027] Such methods can be iteratively repeated at each of a plurality of predetermined times. The sensors can be, for example, radiation or chemical sensors. Each node can be associated at the predetermined time with at least one of a plurality of node groups based, for example, solely on a position of the node, solely on a velocity of the node, or solely on a measure of traffic on the network, based on any combination of position, velocity, and/or network traffic. Associating each node at the predetermined time with at least one of a plurality of node groups can be carried out by the first computer, or by a second computer that is not the first computer, or by a plurality of computers none of which is the first computer.

Claims

1. A method of detecting a source (30) using:

a plurality of nodes (5a-d, 11-25), each node including a sensor capable of collecting data, wherein the sensors are radiation or chemical sensors, and a transmitter configured to transmit at least sensor data collected by the sensor and location data representing at least the location of the node;

a network capable of allowing transmission of data between and among the plurality of nodes and between the plurality of nodes and at least one computer; and

a first computer (2) having an input configured to receive data transmitted by nodes through the network, a memory configured to collect data transmitted by the nodes through the network, a processor configured to combine sensor and location data and compare the combined data to a predetermined detection criterion to determine whether a source is detected, and an output;

the method comprising:

collecting, in the first computer (2), location data transmitted through the network from each node to the first computer, the data being associated with a predetermined time;
for each node, associating the node at the predetermined time with at least one of a plurality of node groups based at least in part on at least one of (a) a velocity of the node, and (b) a measure of traffic on the network;
for each node group, determining whether a source has been detected by the node group by combining, in the first computer (2), sensor data and location data collected from the nodes in the group and comparing, in the first computer (2), the combined sensor data and location data to at least one predetermined detection criterion; and
signaling, with the output, at least whether a source (30) has been detected.

2. A method of detecting a source (30) comprising iteratively repeating the method of claim 1 at each of a plurality of predetermined times.

3. The method of any of claims 1-2 wherein each node (5a-d, 11-25) is associated at the predetermined time with at least one of a plurality of node groups based solely on a velocity of the node.

4. The method of any of claims 1-2 wherein each node (5a-d, 11-25) is associated at the predetermined time with at least one of a plurality of node groups based solely on a measure of traffic on the network.

5. The method of any of claims 1-2 wherein each node (5a-d, 11-25) is associated at the predetermined time with at least one of a plurality of node groups based also on a position of the node.

6. The method of any of claims 1-5 wherein associating each node (5a-d, 11-25) at the predetermined time with at least one of a plurality of node groups is carried out by a second computer (3, 4) that is not the first computer (2).

7. The method of any of claims 1-5 wherein associating each node (5a-d, 11-25) at the predetermined time with at least one of a plurality of node groups is carried out by a plurality of secondary computers (3, 4) none of which is the first computer ().

8. The method of any of claims 1-5 wherein associating each node (5a-d, 11-25) at the predetermined time with at least one of a plurality of node groups is carried out by the first computer (2).

9. A system of detecting a source comprising:

a first computer (2) having an input configured to receive data, a memory, a processor, and an output;
wherein the system is configured to:

collect, in the first computer (2), data transmitted through a network from each node of a plurality of nodes (5a-d, 11-25), each node including a sensor capable of collecting data, wherein the sensors are radiation or chemical sensors, the data comprising at least sensor data collected by the sensor and location data representing at least the location of the node, the data being associated with a predetermined time;
for each node (5a-d, 11-25), associate the node at the predetermined time with at least one of a plurality of node groups based at least in part on at least one of (a) a velocity of the node, and (b) a measure of traffic on the network;
for each node group, determine whether a source (30) has been detected by the node group by combining, in the first computer (2), sensor data and location data collected from the nodes in the group and comparing, in the first computer (2), the combined sensor data and location data to at least one predetermined detection criterion; and
signal, with the output, at least whether a source (30) has been detected.

10. The system of claim 9 further configured to associate each node (5a-d, 11-25) at the predetermined time with at least one of a plurality of node groups based solely on a velocity of the node.

11. The system of claim 9 further configured to associate each node (5a-d, 11-25) at the predetermined time with at least one of a plurality of node groups based solely on a measure of traffic on the network.

12. The system of claim 9 further configured to associate each node (5a-d, 11-25) at the predetermined time with at least one of a plurality of node groups based also on a position of the node.

13. The system of any of claims 9 to 12 further comprising at least one secondary computer (3, 4), wherein the at least one secondary computer (3, 4) is configured to associate each node (5a-d, 11-25) at the predetermined time with at least one of a plurality of node groups.

Patentansprüche

1. Verfahren zur Erkennung einer Quelle (30) mittels einer Mehrzahl von Knoten (5a-d, 11-25), wobei jeder Knoten einen Sensor, der zum Sammeln von Daten imstande ist, wobei die Sensoren Strahlungs- und chemische Sensoren sind, und einen Sender umfasst, der so ausgelegt ist, dass er wenigstens vom Sensor gesammelte Sensordaten und Standortdaten sendet, die wenigstens den Standort des Knotens darstellen;
eines Netzwerks, das zum Zulassen von Übertragung von Daten zwischen und unter der Mehrzahl von Knoten und zwischen der Mehrzahl von Knoten und mindestens einem Computer imstande ist; und
eines ersten Computers (2) mit einem Eingang, der zum Empfangen von Daten ausgelegt ist, die von Knoten durch das Netzwerk gesendet werden, einem Speicher, der zum Sammeln von Daten ausgelegt ist, die von den Knoten durch das Netzwerk gesendet werden, einem Prozessor, der so ausgelegt ist, dass er Sensor- und Standortdaten kombiniert und die kombinierten Daten mit einem vorgegebenen Erkennungskriterium vergleicht, um zu bestimmen, ob eine Quelle erkannt wird, und einem Ausgang;
wobei das Verfahren umfasst:

Sammeln von Standortdaten im ersten Computer (2), die von jedem Knoten durch das Netzwerk an den ersten Computer gesendet werden, wobei die Daten mit einer vorgegebenen Zeit assoziiert sind;
Assoziieren für jeden Knoten des Knotens zu der vorgegebenen Zeit mit mindestens einer von einer Mehrzahl von Knotengruppen wenigstens zum Teil basierend auf mindestens einem von (a) einer Geschwindigkeit des Knotens und (b) einem Verkehrsausmaß im Netzwerk;
Bestimmen für jede Knotengruppe, ob eine Quelle erkannt wurde, durch die Knotengruppe durch Kombinieren von Sensordaten und Standortdaten, die von den Knoten in der Gruppe gesammelt werden, im ersten Computer (2) und Vergleichen der kombinierten Sensordaten und Standortdaten im ersten Computer (2) mit mindestens einem vorgegebenen Erkennungskriterium; und
Signalisieren mit dem Ausgang wenigstens, ob eine Quelle (30) erkannt wurde.

2. Verfahren zur Erkennung einer Quelle (30), umfassend ein iteratives Wiederholen des Verfahrens nach Anspruch 1 zu jeder einer Mehrzahl von vorgegebenen Zeiten.

3. Verfahren nach einem der Ansprüche 1 bis 2, wobei jeder Knoten (5a-d, 11-25) zur vorgegebenen Zeit ausschließlich basierend auf einer Geschwindigkeit des Knotens mit mindestens einer von einer Mehrzahl von Knotengruppen assoziiert wird.

4. Verfahren nach einem der Ansprüche 1 bis 2, wobei jeder Knoten (5a-d, 11-25) zur vorgegebenen Zeit ausschließlich basierend auf einem Verkehrsausmaß im Netzwerk mit mindestens einer von einer Mehrzahl von Knotengruppen assoziiert wird.

5. Verfahren nach einem der Ansprüche 1 bis 2, wobei jeder Knoten (5a-d, 11-25) zur vorgegebenen Zeit auch basierend auf einer Position des Knotens mit mindestens einer von einer Mehrzahl von Knotengruppen assoziiert wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, wobei das Assoziieren jedes Knotens (5a-d, 11-25) zur vorgegebenen Zeit mit mindestens einer von einer Mehrzahl von Knotengruppen von einem zweiten Computer (3, 4) durchgeführt wird, der nicht der erste Computer (2) ist.

7. Verfahren nach einem der Ansprüche 1 bis 5, wobei das Assoziieren jedes Knotens (5a-d, 11-25) zur vorgegebenen Zeit mit mindestens einer von einer Mehrzahl von Knotengruppen von einer Mehrzahl von sekundären Computern (3, 4) durchgeführt wird, von welchen keiner der erste Computer () ist.

8. Verfahren nach einem der Ansprüche 1 bis 5, wobei das Assoziieren jedes Knotens (5a-d, 11-25) zur vorgegebenen Zeit mit mindestens einer von einer Mehrzahl von Knotengruppen vom ersten Computer (2) durchgeführt wird.

9. System zum Erkennen einer Quelle, umfassend:

einen ersten Computer (2) mit einem Eingang, der zum Empfangen von Daten ausgelegt ist, einem Speicher, einem Prozessor und einem Ausgang;
wobei das System ausgelegt ist zum:

Sammeln von Daten im ersten Computer (2), die von jedem Knoten einer Mehrzahl von Knoten (5a-d, 11-25) durch ein Netzwerk gesendet werden, wobei jeder Knoten einen Sensor umfasst, der zum Sammeln von Daten imstande ist, wobei die Sensoren Strahlungs- oder chemische Sensoren sind, die Daten wenigstens vom Sensor gesammelte Sensordaten und Standortdaten umfassen, die wenigstens den Standort des Knotens darstellen, wobei die Daten mit einer vorgegebenen Zeit assoziiert sind;
Assoziieren für jeden Knoten (5a-d, 11-25) des Knotens zu der vorgegebenen Zeit mit

mindestens einer von einer Mehrzahl von Knotengruppen wenigstens zum Teil basierend auf mindestens einem von (a) einer Geschwindigkeit des Knotens und (b) einem Verkehrsausmaß im Netzwerk;
Bestimmen für jede Knotengruppe, ob eine Quelle (30) erkannt wurde, durch die Knotengruppe durch Kombinieren von Sensordaten und Standortdaten, die von den Knoten in der Gruppe gesammelt werden, im ersten Computer (2) und Vergleichen der kombinierten Sensordaten und Standortdaten im ersten Computer (2) mit mindestens einem vorgegebenen Erkennungskriterium; und
Signalisieren mit dem Ausgang wenigstens, ob eine Quelle (30) erkannt wurde.

10. System nach Anspruch 9, ferner ausgelegt zum Assoziieren jedes Knotens (5a-d, 11-25) zur vorgegebenen Zeit ausschließlich basierend auf einer Geschwindigkeit des Knotens mit mindestens einer von einer Mehrzahl von Knotengruppen.

11. System nach Anspruch 9, ferner ausgelegt zum Assoziieren jedes Knotens (5a-d, 11-25) zur vorgegebenen Zeit ausschließlich basierend auf einem Verkehrsausmaß im Netzwerk mit mindestens einer von einer Mehrzahl von Knotengruppen.

12. System nach Anspruch 9, ferner ausgelegt zum Assoziieren jedes Knotens (5a-d, 11-25) zur vorgegebenen Zeit auch basierend auf einer Position des Knotens mit mindestens einer von einer Mehrzahl von Knotengruppen.

13. System nach einem der Ansprüche 9 bis 12, ferner umfassend mindestens einen sekundären Computer (3, 4), wobei der mindestens eine sekundäre Computer (3, 4) so ausgelegt ist, dass er jeden Knoten (5a-d, 11-25) zur vorgegebenen Zeit mit mindestens einer von einer Mehrzahl von Knotengruppen assoziiert.

Revendications

1. Procédé de détection d'une source (30) au moyen :

d'une pluralité de nœuds (5a-d, 11-25), chaque nœud comportant un capteur pouvant collecter des données, les capteurs étant des capteurs de rayonnement ou chimiques, et un émetteur configuré pour transmettre au moins des données de capteur collectées par le capteur et des données d'emplacement représentant au moins l'emplacement du nœud ;
d'un réseau pouvant autoriser la transmission de données entre et parmi la pluralité de nœuds et entre la pluralité de nœuds et au moins un ordinateur ; et
d'un premier ordinateur (2) ayant une entrée configurée pour recevoir des données transmises par des nœuds à travers le réseau, une mémoire configurée pour collecter des données transmises par les nœuds à travers le réseau, un processeur configuré pour combiner des données de capteur et d'emplacement et comparer les données combinées à un critère de détection prédéterminé pour déterminer si une source est détectée, et une sortie ;
le procédé comprenant :

la collecte, dans le premier ordinateur (2), de données d'emplacement transmises à travers le réseau depuis chaque nœud au premier ordinateur, les données étant associées à un moment prédéterminé ;
pour chaque nœud, l'association du nœud au moment prédéterminé avec au moins un d'une pluralité de groupes de nœuds au moins en partie sur la base d'au moins un élément parmi (a) une vitesse du nœud, et (b) une mesure de trafic sur le réseau ;
pour chaque groupe de nœuds, la détermination qu'une source a été détectée ou non par le groupe de nœuds par combinaison, dans le premier ordinateur (2), de données de capteur et de données d'emplacement collectées depuis les nœuds dans le groupe et comparaison, dans le premier ordinateur (2), des données de capteur et données d'emplacement combinées à au moins un critère de détection prédéterminé ; et
le signalement, avec la sortie, au moins qu'une source (30) a été détectée ou non.

2. Procédé de détection d'une source (30) comprenant la répétition itérative du procédé de la revendication 1 à chacun d'une pluralité de moments prédéterminés.

3. Procédé de l'une quelconque des revendications 1 et 2 dans lequel chaque nœud (5a-d, 11-25) est associé au moment prédéterminé avec au moins un d'une pluralité de groupes de nœuds uniquement sur la base d'une vitesse du nœud.

4. Procédé de l'une quelconque des revendications 1 et 2 dans lequel chaque nœud (5a-d, 11-25) est associé au moment prédéterminé avec au moins un d'une pluralité de groupes de nœuds uniquement sur la base d'une mesure de trafic sur le réseau.

5. Procédé de l'une quelconque des revendications 1 et 2 dans lequel chaque nœud (5a-d, 11-25) est as-

socié au moment prédéterminé avec au moins un d'une pluralité de groupes de nœuds également sur la base d'une position du nœud.

6. Procédé de l'une quelconque des revendications 1 à 5 dans lequel l'association de chaque nœud (5a-d, 11-25) au moment prédéterminé avec au moins un d'une pluralité de groupes de nœuds est réalisée par un deuxième ordinateur (3, 4) qui n'est pas le premier ordinateur (2).

7. Procédé de l'une quelconque des revendications 1 à 5 dans lequel l'association de chaque nœud (5a-d, 11-25) au moment prédéterminé avec au moins un d'une pluralité de groupes de nœuds est réalisée par une pluralité d'ordinateurs secondaires (3, 4) dont aucun n'est le premier ordinateur ().

8. Procédé de l'une quelconque des revendications 1 à 5 dans lequel l'association de chaque nœud (5a-d, 11-25) au moment prédéterminé avec au moins un d'une pluralité de groupes de nœuds est réalisée par le premier ordinateur (2).

9. Système de détection d'une source comprenant :

un premier ordinateur (2) ayant une entrée configurée pour recevoir des données, une mémoire, un processeur, et une sortie ;
le système étant configuré pour :

collecter, dans le premier ordinateur (2), des données transmises à travers un réseau depuis chaque nœud d'une pluralité de nœuds (5a-d, 11-25), chaque nœud comportant un capteur pouvant collecter des données, les capteurs étant des capteurs de rayonnement ou chimiques, les données comprenant au moins des données de capteur collectées par le capteur et des données d'emplacement représentant au moins l'emplacement du nœud, les données étant associées à un moment prédéterminé ;
pour chaque nœud (5a-d, 11-25), associer le nœud au moment prédéterminé avec au moins un d'une pluralité de groupes de nœuds au moins en partie sur la base d'au moins un élément parmi (a) une vitesse du nœud, et (b) une mesure de trafic sur le réseau ;
pour chaque groupe de nœuds, déterminer si une source (30) a été détectée par le groupe de nœuds en combinant, dans le premier ordinateur (2), des données de capteur et des données d'emplacement collectées depuis les nœuds dans le groupe et en comparant, dans le premier ordinateur (2), les données de capteur et données d'emplacement combinées à au moins un critère de détection prédéterminé ; et
signaler, avec la sortie, au moins si une source (30) a été détectée.

10. Système de la revendication 9 également configuré pour associer chaque nœud (5a-d, 11-25) au moment prédéterminé avec au moins un d'une pluralité de groupes de nœuds uniquement sur la base d'une vitesse du nœud.

11. Système de la revendication 9 également configuré pour associer chaque nœud (5a-d, 11-25) au moment prédéterminé avec au moins un d'une pluralité de groupes de nœuds uniquement sur la base d'une mesure de trafic sur le réseau.

12. Système de la revendication 9 également configuré pour associer chaque nœud (5a-d, 11-25) au moment prédéterminé avec au moins un d'une pluralité de groupes de nœuds également sur la base d'une position du nœud.

13. Système de l'une quelconque des revendications 9 à 12 comprenant en outre au moins un ordinateur secondaire (3, 4), l'au moins un ordinateur secondaire (3, 4) étant configuré pour associer chaque nœud (5a-d, 11-25) au moment prédéterminé avec au moins un d'une pluralité de groupes de nœuds.

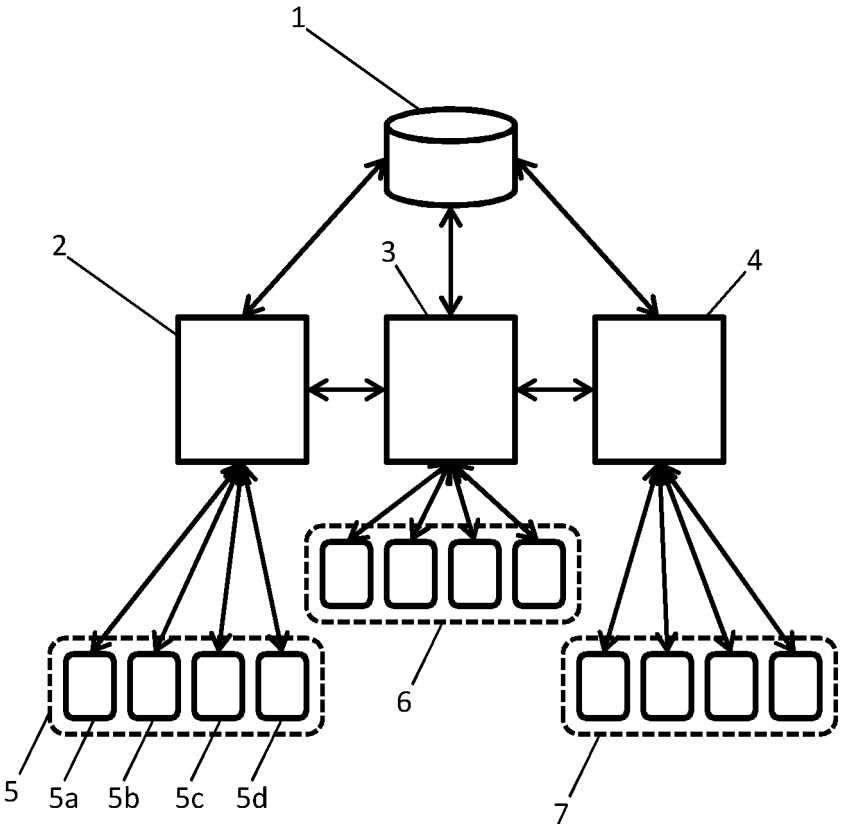

FIG. 1

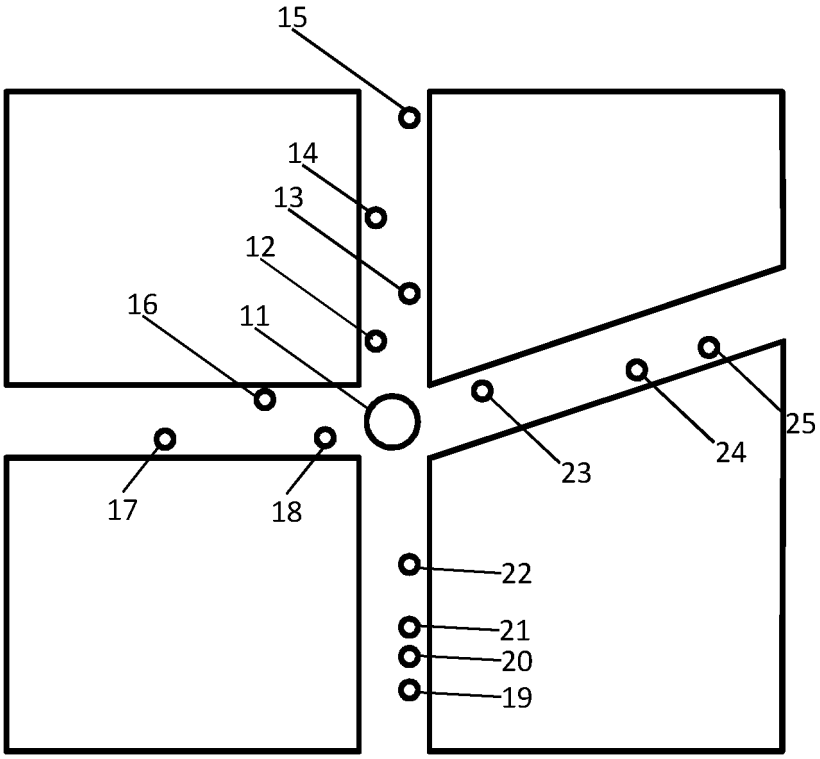

FIG. 2

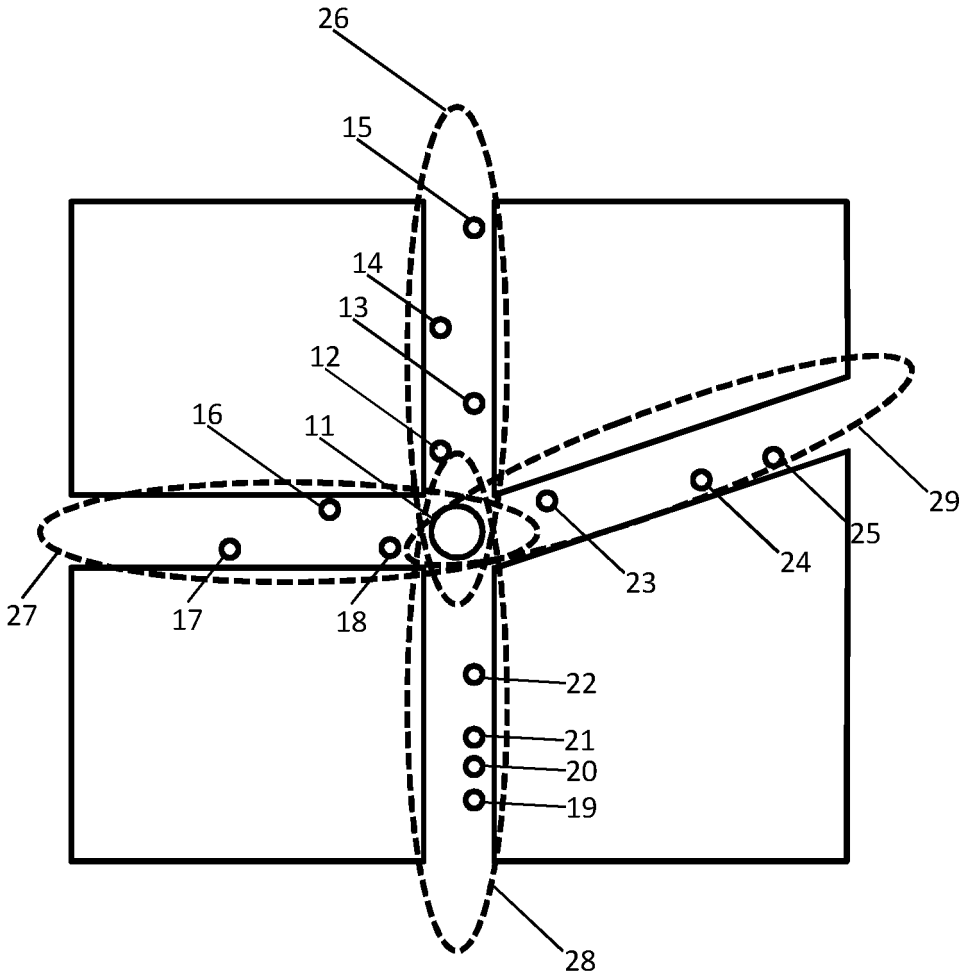

FIG. 3

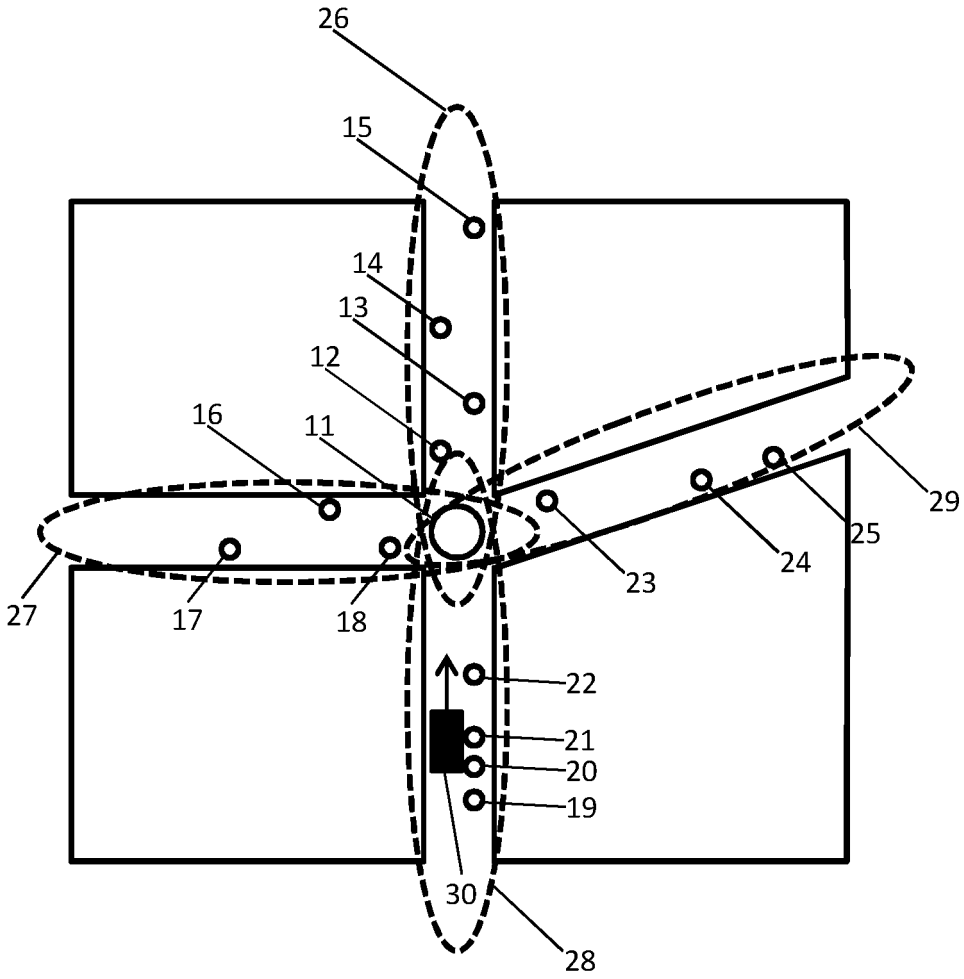

FIG. 4

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 2014012330 W **[0003]**
- WO 20140133687 A **[0003] [0012] [0013] [0019]**
- US 20170003404 A **[0003]**
- CN 103546966 **[0006]**
- WO 2004051868 A **[0007]**
- US 2014099882 A **[0008]**

Non-patent literature cited in the description

- **KOUTSOUKOS XENOFON et al.** OASiS: A Service-Oriented Architecture for Ambient-Aware Sensor Networks. *Medical Image Computing and Computer-Assisted Intervention - MICCAI,* 2015 **[0005]**