(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 January 2014 (03.01.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/000161 A1

(51) International Patent Classification: *H04W 84/18* (2009.01)

(21) International Application Number: PCT/CN2012/077547

(22) International Filing Date: 26 June 2012 (26.06.2012)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **RENESAS MOBILE CORPORATION** [JP/JP]; 6-2, Otemachi, 2-chome, Chiyoda-ku, Tokyo 100-0004 (JP).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **XU, Kenan** [CA/CN]; Room 14-1101, Hai Zhou Li Yuan, 68 Liyuan Road, Huangpu District, Shanghai 200135 (CN). **WANG, Haifeng** [FI/CN]; Room 101, Num 15, Lane 69, Gubei Road, Changning District, Shanghai 200051 (CN). **FENG, Xianjun** [CN/CN]; Room 404, No. 65, Lane 310, Lianhua Road, Minhang District, Shanghai 201102 (CN).

(74) Agent: **KING & WOOD MALLESONS LAWYERS**; 20th Floor, East Tower, World Financial Centre, No. 1 Dongsanhuan Zhonglu, Chaoyang District, Beijing 100020 (CN).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

(54) Title: APPARATUS AND METHOD FOR COOPERATIVE ELECTRONIC DATA COLLECTION

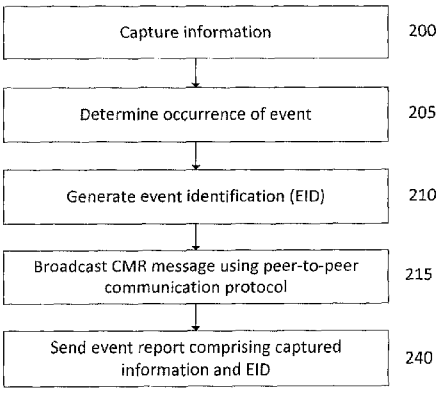

Fig. 2A

(57) Abstract: Embodiments include methods for cooperative, de-centralized data collection among electronic devices, and devices and systems embodying such methods. When a device determines the occurrence of an event, it generates a unique event ID (EID), used to associate all data related to the event. The device broadcasts a request message, comprising the EID and optionally an event description event and requested action(s), to proximate devices. The requested actions may comprise instructions for monitoring the event and reporting information to a central repository. When a device receives the request message, it responds according to the requested actions and any other information in the message. The initiating and receiving devices may send event report messages, comprising the EID and captured information, to the repository, which may further process the information received from the devices, using the EID to aggregate all information relevant to the event.

WO 2014/000161 A1

APPARATUS AND METHOD FOR COOPERATIVE ELECTRONIC DATA COLLECTION

TECHNICAL FIELD

5 **[0001]** The disclosure herein relates to the field of device-to-device (D2D) or machine-to-machine (M2M) communications, and more particularly to improvements to cooperative electronic data collection and surveillance system by use of D2D or M2M communications.

BACKGROUND

[0002] In recent years, electronic surveillance systems have been widely adopted by 10 governments and law enforcement agencies for variety of applications related to maintaining social control, recognizing and monitoring threats, and preventing and/or discouraging violations of laws and ordinances. One of the most familiar electronic surveillance applications is the traffic enforcement camera. Although these cameras are most often mounted in fixed locations along roadsides or in intersections, they also may be installed in 15 movable enforcement vehicles, such as police cars. Traffic enforcement cameras are often used to detect traffic violations such as exceeding the posted speed limit, failure to stop for a traffic light or stop sign, and unauthorized use of a restricted lane. However, such cameras also may be used for recording identifying vehicular information (e.g., license plate) for purposes of billing the driver for usage of toll roads, toll areas, etc.

20 **[0003]** Closed-circuit television (CCTV) is another exemplary electronic surveillance system that is in widespread use. CCTV differs from "broadcast" TV in that the signal is not openly transmitted, though it may employ point to point (P2P), point to multipoint, or mesh wireless links. CCTV is most often used for surveillance and monitoring in areas such as banks, casinos, airports, public transportation, military installations, and convenience stores. 25 CCTV surveillance systems have been widely deployed throughout the United Kingdom (UK), where various estimates for the total number of CCTV cameras range between 1,850,000 and 4,200,000. Police officials (e.g., Metropolitan Police) often use CCTV recordings from various sources for tracing the movements of suspects or victims of crimes, and anti-terrorist officers often use CCTV recordings to track terrorist suspects. Similarly, 30 the city of Chicago operates a networked CCTV surveillance system which combines video

captured by government and private-sector cameras, including those installed in city buses, businesses, public schools, subway stations, housing projects, etc. Other private-sector applications of CCTV include monitoring of industrial processes that take place under conditions dangerous for humans, such as those found in the manufacturing of certain chemicals and nuclear fuel.

[0004] Individuals and businesses also have adopted electronic surveillance systems for other monitoring and protection applications. For example, an event data recorder (EDR) is a device installed in some automobiles to record information related to vehicle crashes or accidents. In modern diesel trucks, EDRs are triggered by electronically sensed problems in the engine (often called faults), or a sudden change in wheel speed. Information from these devices can be collected after a crash and analyzed to help determine what the vehicles were doing before, during and after the crash or event. Some EDRs – called video EDRs (VEDRs) – may also include a video recorder that can be running continuously or triggered to start under various conditions. Typically, a VEDR records only video from the front view from the car, which is sufficient to capture some types of accidents but not those occurring from the side or rear of the car.

[0005] Conventionally, most electronic surveillance systems are either isolated systems at fixed locations or operate for dedicated purpose(s). For example, while traffic enforcement cameras effectively record images of vehicles failing to stop for a traffic light at an intersection, they are not deployed nor configured for recording scenes of an accident at that same intersection. By further example, although a VEDR installed in a personal vehicle may be triggered to begin recording an accident involving that vehicle, it is not operable to record other events in the vicinity that do not directly involve that vehicle. Even when electronic surveillance systems allow for some degree of cooperation among surveillance devices, both the functionality and the benefit of the cooperation are usually limited. Moreover, such problems are common not only to surveillance systems but also to other types of electronic data collection systems, such as wireless sensor networks.

SUMMARY

[0007] Embodiments of the present disclosure include methods for cooperative, de-centralized data collection (e.g., surveillance or sensing) among a plurality of fixed and/or mobile electronic devices, and electronic devices embodying such methods. When an

electronic device determines the occurrence of an event, it generates a globally unique event ID (EID), which is used to associate all data generated by the plurality of electronic devices related to the event. The initiating electronic device broadcasts a cooperative monitoring request (CMR) message, also comprising the EID, to all other electronic devices its local proximity. The CMR message may comprise a description of the nature or type of the event and one or more actions requested of the receiving electronic devices. In some embodiments, the one or more requested actions may comprise instructions for monitoring the detected event and/or reporting information related to the event to a central repository. In some embodiments, the initiating electronic device sends an event report message, also comprising the EID, to a central repository. When a nearby electronic device receives the CMR message, it responds according to the requested actions and any other information in the message. In some embodiments, the receiving electronic device sends one or more event report messages, also comprising the EID received in the CMR message, to the central repository. In some embodiments, the central repository may further process the information received from the electronic devices, using the EID to search for and collect all information relevant to the event.

[0008] Embodiments also include an electronic data collection system, comprising a plurality of electronic devices, each comprising a transmitter and a receiver, and a central repository, comprising a database for storing information. The plurality of electronic devices is communicably coupled via a peer-to-peer wireless communication protocol, and the central repository is communicably coupled to the plurality of electronic devices. At least one of the plurality of electronic devices is operable to transmit a request message directed to the remainder of the plurality of electronic devices, the request message comprising an event identification (EID). In some embodiments, the request message comprises at least one command. At least one of the remainder of the plurality of electronic devices is operable to receive the request message, capture information in response to the command, and transmit a report message to the central repository, each report message comprising the event identification (EID) and at least a portion of the information captured by the respective one of the remainder of the plurality of electronic devices.

DESCRIPTION OF THE DRAWINGS

[0009] The detailed description will refer to the following drawings, wherein like numerals refer to like elements, and wherein:

Fig. 1 is diagram of a scenario taking place at an intersection that illustrates the operation of certain embodiments of the present disclosure;

Fig. 2A is a flowchart of an exemplary cooperative data collection method for an electronic device according to one or more embodiments of the present disclosure;

Fig. 2B is a flowchart of another exemplary cooperative data collection method for an electronic device according to one or more embodiments of the present disclosure;

Fig. 3 is a flowchart of another exemplary cooperative data collection method for an electronic device, according to one or more embodiments of the present disclosure;

Fig. 4A is a diagram of an exemplary structure of an event report message according to one or more embodiments of the present disclosure;

Fig. 4B is a diagram of an exemplary structure of a cooperative monitoring request (CMR) message according to one or more embodiments of the present disclosure; and

Fig. 5 is a block diagram of an exemplary electronic device according to one or more embodiments of the present disclosure; and

DETAILED DESCRIPTION

[0010] Several attempts have been made at improving either the effectiveness of the individual surveillance devices or cooperative efficiency of the individual devices within a surveillance system. For example, U. S. Patent Pub. No. 2009/0115848 discloses an improved, multi-directional traffic image capturing system comprising one forward direction camera and two side direction cameras, collocated and under common control. Likewise, U. S. Patent No. 7,804,981 discloses an improved electronic surveillance system for tracking an object (e.g., an airplane) in the vicinity of an airport. The system includes one or more non-imaging surveillance devices (NSDs) at fixed, known locations that are used to determine the position of the object of interest. The system also includes one or more imaging surveillance devices (ISDs) at fixed, known locations that are used to capture image data for the object of interest at the position determined by the NSD(s).

[0011] U. S. Patent Pub. No. 2004/0216165 discloses a centralized, cooperative surveillance system comprising two or more surveillance terminals and a surveillance center. The terminals and the center are connected via a network. If a terminal detects a hazard, it

sends a hazard signal to the center. The center then sends a cooperative surveillance command to other terminals that are at fixed, known locations (e.g., in homes) in the vicinity of the reported event or hazard, which in turns sends video data to the center.

[0012] Similarly, U. S. Patent No. 7,088,240 discloses a centralized, cooperative surveillance system comprising multiple surveillance terminals and a surveillance center, connected by a network. One of the terminals detects a hazard and sends a signal reporting the detected hazard to the surveillance center. The surveillance center receives the hazard information signal, identifies what the type of hazard and the information source (i.e., location of the sending terminal), and selects other terminals to be alerted based on their known proximity or relationship to the location of the hazard and the type of the hazard reported.

[0013] U. S. Patent No. 7,227,569 discloses a centralized surveillance system in which multiple cameras arranged in known, fixed locations (e.g., within a facility) cooperatively track and monitor an object. According to the disclosure, a surveillance camera acquires images of an object and analyzes the image data to extract feature information. Once the object has moved out of the camera's range, the camera then sends the feature information to other cameras known to be within the system, along with a command to start monitoring for these features.

[0014] Accordingly, even when electronic surveillance systems provide some degree of cooperation among surveillance devices, the cooperation is limited in at least the following ways. First, the cooperative surveillance devices (e.g., CCTV cameras) are positioned at known, stationary locations. Second, the number of surveillance devices in a cooperative electronic surveillance system is often fixed at the time the system is provisioned, making the addition of new devices difficult, time-consuming, and costly. Consequently, even if the number and locations of cooperating surveillance devices are chosen to maximize coverage (e.g., based on population density), certain events will be outside the view of the statically configured electronic surveillance system. On the other hand, if the some of the surveillance devices within the system are mobile, the system must be aware of their locations at all times and in any event, there is no guarantee that their locations will be sufficiently close to events of interest at a particular time.

[0015] Another limitation is that control of these cooperative electronic surveillance systems is usually centralized. So, even if a particular surveillance device captures information (e.g., video) pertaining to an event within its view, central control must receive and process this information prior to directing other nearby surveillance devices to capture additional information. Consequently, such centralized, cooperative electronic surveillance systems may not respond rapidly enough to an event or situation occurring in a small, localized area. This results in inefficient usage of the expensive surveillance system.

[0016] Such problems are not unique to electronic surveillance systems. For example, wireless sensor networks consist of spatially distributed autonomous sensors typically used to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, humidity, motion or pollutants and to cooperatively pass their data through a network to a main location such as a central repository or control station. To the extent that nodes in wireless sensor networks are integrated into devices, vehicles, etc. that are mobile, the same problems exist with respect to determining and tracking their locations quickly enough to timely collect data or capture information related to a particular event of interest. Moreover, in many wireless sensor networks there is no centralized control to track and allocate resources.

[0017] Embodiments of the present disclosure include a system and method for cooperative, de-centralized data collection (e.g., surveillance or sensing) among a plurality of fixed and/or mobile electronic devices. When an electronic device determines the occurrence of an event, it generates a globally unique event ID (EID), which is used to associate all data generated by the plurality of electronic devices related to the event. The initiating electronic device broadcasts a cooperative monitoring request (CMR) message, also comprising the EID, to all other electronic devices its local proximity. The CMR message may comprise a description of the nature or type of the event and one or more actions requested of the receiving electronic devices. In some embodiments, the one or more requested actions may comprise instructions for monitoring the event and/or reporting information related to the event to a central repository.

[0018] In some embodiments, the initiating electronic device sends an event report message, also comprising the EID, to a central repository. In some embodiments, the initiating electronic device sends the event report message substantially contemporaneous with

completion of capturing information associated with an EID. In other embodiments, the initiating electronic device stores all captured information associated with one or more EIDs until a later time, when it transfers the captured information associated with the one or more EIDs to the central repository using, for example, one or more event report messages. The later time may be predetermined, in response to an external request, or at the discretion or convenience of the sending device. In some embodiments, the stored captured information may be marked as protected in the memory where it is stored to prevent deletion and/or overwrite.

[0019] When a nearby electronic device receives the CMR message, it responds according to the requested actions and any other information in the message. In some embodiments, the receiving electronic device sends one or more event report messages, also comprising the EID received in the CMR message, to the central repository. In some embodiments, the receiving electronic device sends the event report message substantially contemporaneous with completion of capturing information associated with an EID. In other embodiments, the receiving electronic device stores all captured information associated with one or more EIDs until a later time, when it sends the captured information associated with the one or more EIDs in one or more event report messages to the central repository. The later time may be predetermined, in response to an external request, or at the discretion or convenience of the sending device. The stored captured information may be marked as protected in the memory where it is stored to prevent deletion and/or overwrite. In some embodiments, the central repository may further process the information received from the electronic devices, using the EID to search for and collect all information relevant to the event.

[0020] Embodiments also include a method for cooperative data collection by an electronic device, comprising receiving a request message related to a proximate event via a peer-to-peer wireless communication protocol, wherein the request messages comprises an event identification (EID); capturing information related to the proximate event using at least one sensor; and transmitting a report message comprising the event identification (EID) and at least a portion of the captured information. In some embodiments, the request message related to the proximate event comprises identifying information for a central repository, and transmitting the report message to the central repository is based on the identifying information. In some embodiments, the report message is transmitted substantially

contemporaneous with the completion of capturing the at least a portion of the captured information included in the report message. In other embodiments, the report message is transmitted at a later time, which may be predetermined, in response to an external request, or at the discretion or convenience of the sending device. In some embodiments, the method further comprises transmitting an acknowledgement (ACK) message via a peer-to-peer wireless communication protocol, wherein the acknowledgement (ACK) message comprises the event identification (EID). Other embodiments include electronic devices and computer-readable media embodying one or more of the above methods.

[0021] Embodiments also include a method for cooperative electronic data collection by an electronic device, comprising capturing information using at least one sensor; determining the occurrence of an event based on the captured information; associating an event identification (EID) with the captured information; transmitting a request message via at least one peer-to-peer wireless communication protocol, wherein the request message comprises the event identification (EID); and transmitting a report message to a central repository, wherein the report message comprises the event identification (EID) and at least a portion of the captured information. In some embodiments, the report message is transmitted substantially contemporaneous with the completion of capturing the at least a portion of the captured information included in the report message. In other embodiments, the report message is transmitted at a later time, which may be predetermined, in response to an external request, or at the discretion or convenience of the sending device. In some embodiments, the method comprises repeatedly transmitting the request message via the at least one wireless communication protocol until either reaching a maximum number of transmissions or receiving an acknowledgement (ACK) message. Other embodiments include electronic devices and computer-readable media embodying one or more of the above methods.

[0022] Other embodiments include an electronic data collection system, comprising a plurality of electronic devices, each comprising a transmitter and a receiver, and a central repository, comprising a database for storing information. The plurality of electronic devices is communicably coupled via a peer-to-peer wireless communication protocol. The central repository is communicably coupled to the plurality of electronic devices. At least one of the plurality of electronic devices is operable to transmit a request message directed to the

remainder of the plurality of electronic devices, the request message comprising an event identification (EID) and, optionally, a command. At least one of the remainder of the plurality of electronic devices is operable to receive the request message, capture information in response to the command, and transmit a report message to the central repository, each report message comprising the event identification (EID) and at least a portion of the information captured by the respective one of the remainder of the plurality of electronic devices. The central repository is operable to receive report messages from the plurality of electronic devices and to store the captured information comprising the report messages in association with the event identification (EID).

[0023] Fig. 1 is diagram of a scenario taking place at an intersection that illustrates the operation of certain embodiments of the system and method of the present disclosure. Each of vehicles 101, 102, 103, and 104 are equipped with electronic devices 111, 112, 113, and 114, each comprising a camera. In the exemplary embodiments described with respect to Fig. 1, electronic devices 111, 112, 113, and 114 are surveillance devices. However, electronic devices 111, 112, 113, and 114 may be wireless sensing devices (e.g., nodes in a wireless sensor network) in other embodiments within the scope of the present disclosure.

[0024] Traffic signals 107 and 108 are positioned in a customary manner on roadside poles diagonally across intersection 105 from each other, controlling traffic in direction 120. Each of traffic signals 107 and 108 is displaying a red light, indicating that traffic through the intersection in direction 120 is prohibited at this time. Surveillance device 106, comprising a traffic violation camera, also is positioned at intersection 105 to detect violations of traffic signals 107 and 108 (i.e., in direction 120).

[0025] As shown in Fig. 1, vehicle 104 passes through intersection 105 in violation of the red light condition presently displayed on traffic signals 107 and 108. Surveillance device 106 detects this violation by vehicle 104 and captures the relevant image data, e.g., of the license plate of vehicle 104. In some situations, the image captured by surveillance device 106 may not be sufficiently clear due to bad weather, poor visibility, debris covering the license plate, etc. Moreover, even if the image captured by surveillance device 106 is sufficient for establishing liability for a traffic signal violation, it may not be sufficient to establish other liability related to this event, such as the cause(s) of a collision between vehicle 104 and another vehicle or a pedestrian. Accordingly, it would be advantageous to

utilize the surveillance cameras on nearby vehicles 101, 102, and 103 to capture additional images, video, audio, or other information about the event taking place at intersection 105. If available, this additional information may be used by law enforcement, insurance companies, or other concerned parties to better reconstruct the events taking place at intersection 105, and to determine any liability arising therefrom.

[0026] According to embodiments of the present disclosure, when surveillance device 106 detects a violation of traffic signals 107 and 108 by vehicle 104, it assigns a unique EID to the violation and broadcasts a CMR message, comprising the EID, to all other surveillance devices its vicinity. As used herein, the terms "broadcast" and "broadcasting" may comprise broadcasting, multicasting, sending multiple unicasts, or a combination thereof, to at least one proximate device. Moreover, the term "unique EID" is used herein to mean either that the EID is different than any other EIDs or if the EID is the same as another EID in the cooperative electronic surveillance system, the distinction between the two can be resolved by reference to other information (e.g., time or place of origin).

[0027] In some embodiments, surveillance device 106 broadcasts the CMR message using peer-to-peer radio-frequency communication protocols in licensed or unlicensed spectrum bands, such as Long-Term Evolution (LTE) D2D protocols standardized by the 3rd Generation Partnership Project (3GPP). In some embodiments, surveillance device 106 broadcasts the CMR message using peer-to-peer radio-frequency (e.g., wireless) communication protocols in unlicensed spectrum bands, such as 802.11p protocols standardized by the Institute of Electrical and Electronic Engineers (IEEE), either instead of or in addition to the LTE D2D broadcast. The person of ordinary skill will recognize that these wireless communication protocols are exemplary, and that others (e.g., Bluetooth, RFID) may be used within the scope of the present disclosure. In some embodiments, surveillance device 106 broadcasts the CMR message a fixed number of times or for a fixed duration of time. In some embodiments, surveillance device 106 may broadcast the CMR message repeatedly until it receives responses from one or more other surveillance devices.

[0028] In some embodiments, the CMR message may comprise commands or instructions for monitoring the event and reporting information related to the event to a central repository 130. In some embodiments, the CMR message comprises an identifier or address for central repository 130, such as an Internet Protocol (IP) address. In some embodiments, the CMR

message comprises the time and/or location of the event's occurrence. In some embodiments, the CMR message comprises information identifying the type of event. Surveillance device 106 also may send an event report (ER) message, also comprising the EID, to central repository 130 using one or more of the radio-frequency communication protocols mentioned above, or by a wired connection to central repository 130 through a public or private network. In some embodiments, central repository 130 comprises a relational database storage system.

[0029] One or more of surveillance devices 111, 112, and 113 located, respectively, in vehicles 101, 102, and 103 may receive the CMR message broadcast by surveillance device 106, provided that they are within range and are operating using the same protocol in the same spectrum band as surveillance device 106. By way of example, surveillance devices 111 and 112 receive the CMR message broadcast by surveillance device 106. Upon receipt of the CMR message, each of surveillance devices 111 and 112 determine the EID, commands and instructions, and other fields included in the message. In some embodiments, at least one of surveillance devices 111 and 112 sends an acknowledgement (ACK) message to the initiating surveillance device 106 in response to the CMR message.

[0030] In some embodiments, the CMR message may comprise a command to capture still images, video, audio, or other information. In some embodiments, the CMR message may comprise a set of capture parameters, such as capture duration before and/or after the event, frame rate, sample rate, resolution, duration to keep captured data in memory, etc. In some embodiments, the CMR message may comprise information relating to priorities for transmitting the particular EID and its associated captured information to a central repository. In some embodiments, the CMR message may comprise a command to propagate the CMR request message further using the peer-to-peer wireless communication protocol, e.g., by using multi-hop flooding. In such case, the command may specify how far (i.e., the number of additional hops) to propagate the message. In some embodiments, the CMR message may comprise the location and/or time of the event identified by the EID included in the message. The CMR message may comprise a combination of these and other fields and commands within the scope of the present disclosure.

[0031] In the exemplary embodiment illustrated in Fig. 1, the CMR message comprises a capture command and an associated set of capture parameters. In response to receiving this command, surveillance devices 111 and 112 activate their cameras and/or other sensors and

begin recording still images, video, audio, or other information, according to the capabilities of surveillance devices 111 and 112 and the content of the command. In the case where the surveillance devices 111 and 112 are already actively capturing information, they may adjust the parameters of the ongoing information capture (e.g., sample rate, frame rate, resolution, etc.) to comply with the received capture command.

[0032] In some embodiments, at least one of surveillance devices 111 and 112 stores the recorded still images or video in a file in a memory, and sends the recorded file to central repository 130 after completing recording. In other embodiments, at least one of surveillance devices 111 and 112 establishes a streaming connection to central repository 130 (e.g., by SIP, RTSP, and RTP protocols known to persons of ordinary skill) and streams the captured images or video to central repository 130. In both the store-and-send and the streaming embodiments, surveillance devices 111 and 112 associate the EID received from surveillance device 106 with the file or stream, respectively, sent to central repository 130. Central repository 130 stores the information received from each of surveillance devices 106, 111, and 112 in association with the EID. In this manner, information related to the event associated with the EID can be easily searched and located from among all the information contained with central repository 130.

[0033] Surveillance devices can associate the EID with the captured information provided to central repository 130 in various ways. In some embodiments, surveillance devices include both the EID and the captured information as fields in a message sent to central repository 130. In streaming embodiments, the surveillance devices may associate the EID with the captured information during stream setup, e.g., by using RTSP directives such as DESCRIBE and ANNOUNCE. In some embodiments, the surveillance devices may include the EID in the name of the file comprising the captured information, or in the name of a directory including all captured information files associated with the EID. In some embodiments, surveillance devices may embed the EID as metadata in the captured information. Persons of ordinary skill will recognize that a combination of these or other methods may be used within the scope of the present disclosure.

[0034] Fig. 2A is a flowchart of an exemplary cooperative data collection method for an electronic device, such as electronic device 500 described below with reference to Fig. 5, according to one or more embodiments of the present disclosure. Although the blocks in Fig.

2 are shown in a particular order from top to bottom, this order is merely exemplary and persons of ordinary skill will recognize that the functions represented by the respective blocks of Fig. 2 may be executed in a variety of orders within the scope of the present disclosure. In block 200, the electronic device is capturing information using one of more sensors such as a still image camera, a video camera, a microphone, a digital thermometer, a GPS receiver, an accelerometer, a compass, a gyroscope, and other capturing components known to persons of ordinary skill in the art. The electronic device may store all or part of the captured information in a memory that is operably coupled and accessible to the electronic device. The stored captured information also may be marked as protected in the memory where it is stored to avoid deletion and/or overwrite. For example, in some embodiments, the memory may be capable of storing only a fixed number of images or a fixed duration of video, which may comprise the most recently captured images and/or video. In the case that stored captured information is marked as protected, the electronic device may not overwrite such information and may only utilize memory that is free or contains non-protected information for storing newly captured information.

[0035] In block 205, the electronic device determines the occurrence of an event (e.g., a traffic violation), for example, by detecting the event or receiving an indication that an event has been detected, based at least in part on the information captured in block 200. The electronic device may detect the event according to methods known to persons of ordinary skill in the art, such as pattern matching. In block 210, the electronic device assigns a unique event identifier (EID) to the event. The electronic device may determine the EID in various ways including, for example, pseudo-random number generation; combining (e.g., by computing a hash) information comprising the address of the electronic device (e.g., MAC address) and one or more of the time, date, and location of the event; sequentially from a pool of EIDs assigned to the device; or by a combination of these and/or other methods.

[0036] In block 215, the electronic device broadcasts a cooperative monitoring request (CMR) message to other proximate electronic devices using a peer-to-peer wireless communication protocol, such as LTE D2D or 802.11p. The CMR message comprises the EID assigned in block 210 and a capture command, along with one or more other optional fields as illustrated by the exemplary embodiment of Fig. 4B. In block 240, the electronic device sends an event report message to a central repository. The event report comprises the

EID assigned in block 210 and at least a portion of the information captured in block 200, along with one or more other optional fields as illustrated by the exemplary embodiment of Fig. 4A. As described above, the electronic device may send the event report message comprising the EID substantially contemporaneous with completing the capturing of information in block 200, or may delay sending the event report message until a later time, which may be predetermined, in response to an external request (from, e.g., a central repository, an emergency dispatch center, an application server, or another external source), or at the discretion or convenience of the sending device. In case of delayed sending, the event report message comprising the EID may be coupled or combined with other EIDs and related captured information.

[0037] Fig. 2B is a flowchart of another exemplary cooperative surveillance method for an electronic device, such as electronic device 500 described below with reference to Fig. 5, according to one or more embodiments of the present disclosure. Although the blocks in Fig. 2 are shown in a particular order from top to bottom, this order is merely exemplary and persons of ordinary skill will recognize that the functions represented by the respective blocks may be executed in a variety of orders within the scope of the present disclosure. Blocks 200, 205, 215, and 240 of Fig. 2B are substantially identical to the respectively numbered blocks described above with reference to Fig. 2A. Block 210 comprises the same functionality described above with reference to block 210 of Fig. 2A, but in block 210 of Fig. 2B, the electronic device also initializes the broadcast counter, N, and ACK counter, M, to zero. Although Fig. 2B shows an embodiment utilizing both a broadcast counter and an ACK counter, the person of ordinary skill will recognize that either counter may be disabled within the scope of the present disclosure.

[0038] After broadcasting the CMR message in block 215, the electronic device proceeds to block 220, where it increments the broadcast counter, N. In block 225, the electronic device determines whether or not it received an acknowledgement (ACK) message from another electronic device in response to the CMR message broadcast in block 215. If an acknowledgement (ACK) message was not received, then the electronic device proceeds to block 235. If an acknowledgement (ACK) message was received, then the electronic device proceeds to block 230 where it increments the ACK counter, M, before proceeding to block 235. The electronic device determines in block 235 whether a minimum number of

acknowledgement (ACK) messages have been received from other electronic devices and whether the broadcast counter, N, is less than the maximum number of broadcast repetitions allowed. If both conditions are true, the electronic device returns to block 215 where it broadcasts another CMR message. If either of the conditions is false, then the electronic device proceeds to block 240. As will be recognized by persons of ordinary skill in the art, the minimum number of acknowledgement messages and the maximum number of broadcast repetitions may be set to any value, including one, within the scope of the present disclosure.

[0039] Fig. 3 is a flowchart of another exemplary cooperative surveillance method for an electronic device, according to one or more embodiments of the present disclosure. Although the blocks in Fig. 3 are shown in a particular order from top to bottom, this order is merely exemplary and persons of ordinary skill will recognize that the functions represented by the respective blocks shown in Fig. 3 may be executed in a variety of orders within the scope of the present disclosure. In block 300, the electronic device receives a cooperative monitoring request (CMR) message from another proximate surveillance via a peer-to-peer wireless communication protocol, such as LTE D2D or 802.11p. The CMR message comprises an event identifier (EID) and a capture command, along with one or more other optional fields as illustrated by the exemplary embodiment of Fig. 4B. In block 305, the electronic device optionally sends an acknowledgement (ACK) message to the sending electronic device via the same peer-to-peer wireless communication protocol. The acknowledgement (ACK) message may comprise the EID.

[0040] In block 310, the electronic device captures information according to the capture command in the CMR message received in block 300. In some embodiments, the electronic device may initiate capturing information in block 310 (e.g., by turning on one or more sensors, such as a camera), while in other embodiments the electronic device may alter ongoing information capture to comply with the parameters of the capture command, as discussed above. The electronic device may store all or part of the captured information in a memory. The stored captured information also may be marked as protected in the memory where it is stored to avoid deletion and/or overwrite. For example, in some embodiments, the memory may be capable of storing only a fixed number of images or a fixed duration of video, which may comprise the most recently captured images and/or video. In the case that stored captured information is marked as protected, the electronic device may not overwrite

such information and may only utilize memory that is free or contains non-protected information for storing newly captured information.

[0041] In block 315, the electronic device sends an event report message comprising the EID that was included in the CMR message received in block 300 and at least a portion of the information captured in block 310, along with one or more other optional fields as illustrated by the exemplary embodiment of Fig. 4A. In some embodiments, the event report message may comprise streamed captured information. In other embodiments, the event report message may comprise captured information stored as a file in the electronic device, instead of or in addition to the streamed capture information. As described previously, the electronic device may send the event report message comprising the EID substantially contemporaneous with completing the capturing of information in block 310, or may delay sending the event report message until a later time, which may be predetermined, in response to an external request (from, e.g., a central repository, an emergency dispatch center, an application server, or another external source), or at the discretion or convenience of the sending device. In case of delayed sending, the event report message comprising the EID may be coupled or combined with other EIDs and related captured information.

[0042] Fig. 4A is a diagram of an exemplary structure of an event report message according to one or more embodiments of the present disclosure. The event report message comprises at least a unique EID 400 and captured information 415, which may comprise one or more images, video, audio, temperature, humidity, orientation, velocity, and acceleration information. Optionally, the event report message may comprise a time of capture field 405 and/or a location of capture field 410, representing respectively the time and location at which captured information 415 was captured by the electronic device sending the event report message. In some embodiments, the time of capture field 405 includes date information. In some embodiments, the time of capture field 410 contains abbreviated time information that permits resolution of the actual time of capture within a limited period (e.g., within a two-hour window). In some embodiments, the location of capture field 405 contains abbreviated location information that permits resolution of the actual capture location within a bounded geographical area. Although Fig. 4A shows the EID as a separate field in the event report message, the EID may alternately or additionally be embedded within the captured information (e.g., as metadata) as described above.

[0043] Fig. 4B is a diagram of an exemplary structure of a cooperative monitoring request (CMR) message according to one or more embodiments of the present disclosure. The CMR message comprises a unique EID 400 and, optionally, a commands and parameters field 435, which contains commands and instructions such as the type of information to capture (e.g., images, video, audio, etc.), the duration of capture (e.g., number or duration) before and/or after the event, resolution of captured information (e.g., pixels, sample rate, frame rate, etc.), priority/importance of the captured information, etc. Commands and parameters field 435 also may include a command to propagate the CMR request message using the peer-to-peer wireless communication protocol (e.g., by multi-hop flooding) and may indicate how far the command should be propagated (e.g., number of hops). The CMR also may include a time of event field 420, a location of event field 425, and/or type or class of event field 430, which if present specify respectively the time, location, and type or class (e.g., traffic violation, traffic accident, crime, etc.) of the event to which EID 400 pertains. The CMR message also may include a central repository identifier field 440, which if present provides information (e.g., IP address) identifying a central repository to which electronic devices receiving the CMR message should send event report messages related to EID 400.

[0044] Fig. 5 is a block diagram of exemplary electronic device or apparatus utilizing certain embodiments of the present disclosure, including one or more of the methods described above with reference to the figures. In some embodiments, device 500 comprises an electronic device while in other embodiments device 500 comprises a wireless sensor device (e.g., node in a wireless sensor network). As shown in Fig. 5, device 500 comprises processor 510 which is operably connected to program memory 520 and data memory 530 via bus 570, which may comprise parallel address and data buses, serial ports, or other methods and/or structures known to those of ordinary skill in the art.

[0045] Program memory 520 comprises software code executed by processor 510 that enables device 500 to communicate with one or more other devices using protocols according to various embodiments of the present disclosure, including surveillance communication protocols according to one or more embodiments of the present disclosure. Program memory 520 also comprises software code executed by processor 510 that enables device 500 to communicate with one or more other devices using other protocols or protocol layers, either in conjunction with or in addition the surveillance communication protocols

described herein. For example, program memory 520 may include software code comprising the Long-Term Evolution (LTE) PHY, MAC, RLC, and PDCP layer protocols standardized by 3GPP, or improvements thereto including improvements relating to peer-to-peer communications (e.g., D2D and/or M2M). By further example, program memory 520 may include software code comprising 802.11 wireless local-area network (WLAN) protocols as standardized by the Institute of Electrical and Electronic Engineers (IEEE), or improvements thereto including 802.11p for Wireless Access in Vehicular Environments. Moreover, program memory 520 may comprise executable software code for other protocols utilized in conjunction with radio transceiver 540, user interface 550, host interface 560, and/or sensors 580. Program memory 520 further comprises software code executed by processor 510 to control the functions of device 500, including configuring and controlling various components such as radio transceiver 540, user interface 550, host interface 560, and/or sensors 580. Such software code may be specified or written using any known or future developed programming language, such as e.g. Java, C++, C, and Assembler, as long as the desired functionality, e.g., as defined by the implemented method steps, is preserved.

[0046] Data memory 530 may comprise memory area for processor 510 to store variables used in protocols, configuration, control, and other functions of device 500. As such, program memory 520 and data memory 530 may comprise non-volatile memory (e.g., flash memory, hard drive, tape drive, etc.), volatile memory (e.g., static or dynamic RAM), or a combination thereof. Moreover, data memory 530 may comprise memory area for processor 510 to store data and information captured from sensors 580. Persons of ordinary skill in the art will recognize that processor 510 may comprise multiple individual processors (not shown), each of which implements a portion of the functionality described above. In such case, multiple individual processors may be commonly connected to program memory 520 and data memory 530 or individually connected to multiple individual program memories and or data memories. More generally, persons of ordinary skill in the art will recognize that various protocols and other functions of device 500 may be implemented in many different combinations of hardware and software including, but not limited to, application processors, signal processors, general-purpose processors, multi-core processors, ASICs, fixed digital circuitry, programmable digital circuitry, analog baseband circuitry, radio-frequency circuitry, software, firmware, and middleware.

[0047] Radio transceiver 540 may comprise radio-frequency transmitter and/or receiver functionality that enables device 500 to communicate with other equipment supporting like wireless communication standards. In an exemplary embodiment, radio transceiver 540 includes a transmitter and a receiver that enable device 500 to communicate with other LTE devices and/or networks that are compatible with relevant 3GPP standards. In some embodiments, radio transceiver 540 is capable of communicating on a plurality of LTE frequency-division-duplex (FDD) frequency bands 1 through 25, as specified in 3GPP standards. In some embodiments, radio transceiver 540 is capable of communicating on a plurality of LTE time-division-duplex (TDD) frequency bands 33 through 43, as specified in 3GPP standards. In some embodiments, radio transceiver 540 is capable of communicating on a combination of these LTE FDD and TDD bands, as well as other bands that are specified in the 3GPP standards. In other embodiments, radio transceiver 540 comprises transmitter and receiver circuitry that enables it to communicate in one or more unlicensed frequency bands, such as the ISM band in the region of 2.4 GHz, with other devices that are compatible with the IEEE 802.11 WLAN standards. For example, radio transceiver 540 may comprise circuitry that enables device 500 to communicate directly with peer devices based on the 802.11p standard. The radio functionality particular to each of these embodiments may be coupled with or controlled by other circuitry in device 500, such as processor 510 executing protocol program code stored in program memory 520.

[0048] User interface 550 may take various forms depending on the particular embodiment of device 500. In some embodiments, device 500 is a mobile phone, in which case user interface 550 may comprise a microphone, a loudspeaker, slidable buttons, depressable buttons, a keypad, a keyboard, a display, a touchscreen display, and/or any other user-interface features commonly found on mobile phones. In other embodiments, device 500 is a monitoring device connectable with and/or controlled by a local or remote host computing device. In such embodiments, user interface 550 may be very simple (e.g., a couple of buttons or a small keypad) or may utilize features of the host computing device, such as the host device's display and/or keyboard.

[0049] Host interface 560 of device 500 also may take various forms depending on the particular embodiment of device 500. In embodiments where device 500 is a mobile phone, host interface 560 may comprise a USB interface, an HDMI interface, or the like. In the

embodiments where device 500 is a monitoring capable of being utilized with a host computing device, host interface may be a USB or PCMCIA interface.

[0050] Sensors 580 comprises one or more devices for capturing information external to device 500, such as images, video, audio, temperature, humidity, location, time, orientation, velocity, acceleration, etc. Accordingly, sensors 580 may comprise one or more of a still image camera, a video camera, a microphone, a digital thermometer, a GPS receiver, an accelerometer, a compass, a gyroscope, and other capturing components known to persons of ordinary skill in the art.

[0051] In some embodiments, device 500 may comprise more functionality than is shown in Fig. 5. In some embodiments, device 500 may also comprise functionality such as a media player, Internet browser, email client, etc., and radio transceiver 540 may include circuitry necessary to communicate using additional radio-frequency communication standards including GSM, GPRS, EDGE, UMTS, HSPA, CDMA2000, Bluetooth, GPS, and/or others. Persons of ordinary skill in the art will recognize the above list of features and radio-frequency communication standards is merely exemplary and not limiting to the scope of the present disclosure. Accordingly, processor 510 may execute software code stored in program memory 520 to control such additional functionality.

[0052] As described herein, a device or apparatus may be represented by a semiconductor chip, a chipset, or a (hardware) module comprising such chip or chipset; this, however, does not exclude the possibility that a functionality of a device or apparatus, instead of being hardware implemented, be implemented as a software module such as a computer program or a computer program product comprising executable software code portions for execution or being run on a processor. A device or apparatus may be regarded as a device or apparatus, or as an assembly of multiple devices and/or apparatuses, whether functionally in cooperation with or independently of each other. Moreover, devices and apparatuses may be implemented in a distributed fashion throughout a system, so long as the functionality of the device or apparatus is preserved. Such and similar principles are considered as known to a skilled person.

[0053] More generally, even though the present disclosure and exemplary embodiments are described above with reference to the examples according to the accompanying drawings, it is to be understood that they are not restricted thereto. Rather, it is apparent to those skilled

in the art that the disclosed embodiments can be modified in many ways without departing from the scope of the disclosure herein. Moreover, the terms and descriptions used herein are set forth by way of illustration only and are not meant as limitations. Those skilled in the art will recognize that many variations are possible within the spirit and scope of the disclosure as defined in the following claims, and their equivalents, in which all terms are to be understood in their broadest possible sense unless otherwise indicated.

WHAT IS CLAIMED IS:

1. A method for cooperative data collection by an electronic device, comprising:

receiving a request message related to a proximate event via a peer-to-peer wireless communication protocol, wherein the request messages comprises an event identification (EID);

capturing information related to the proximate event using at least one sensor; and

transmitting a report message comprising the event identification (EID) and at least a portion of the captured information.

2. The method of claim 1, wherein:

the request message related to the proximate event comprises identifying information for a central repository; and

transmitting the report message to the central repository is based on the identifying information.

3. The method of claim 1, wherein the report message is transmitted substantially contemporaneous with the completion of capturing the at least a portion of the captured information included in the report message.

4. The method of claim 1, wherein the report message is transmitted subsequent to completion of capturing the least a portion of the captured information included in the report message, at a time that is one of (a) predetermined, (b) at the convenience or discretion of the electronic device, and (c) responsive to an external request.

5. The method of claim 1, further comprising transmitting an acknowledgement (ACK) message via a peer-to-peer wireless communication protocol, wherein the acknowledgement (ACK) message comprises the event identification (EID).

6. The method of claim 1, wherein:

the request message related to the proximate event comprises a capture command; and

capturing information related to the proximate event is responsive to the capture command.

7. The method of claim 1, wherein the captured information comprises at least one of an image, video, audio, temperature, humidity, location, time, orientation, velocity, and acceleration.

8. The method of claim 1, wherein the peer-to-peer wireless communications protocol comprises one of a Long-Term Evolution (LTE) device-to-device (D2D) protocol, an 802.11p protocol, a Bluetooth protocol, and a radio-frequency ID (RFID) protocol.

9. A method for cooperative electronic data collection by an electronic device, comprising:

capturing information using at least one sensor;

determining the occurrence of an event based on the captured information;

associating an event identification (EID) with the captured information;

transmitting a request message via at least one peer-to-peer wireless communication protocol, wherein the request message comprises the event identification (EID); and

transmitting a report message to a central repository, wherein the report message comprises the event identification (EID) and at least a portion of the captured information.

10. The method of claim 9, wherein the report message is transmitted substantially contemporaneous with the completion of capturing the at least a portion of the captured information included in the report message.

11. The method of claim 9, wherein the report message is transmitted subsequent to completion of capturing the least a portion of the captured information included in the report message, at a time that is one of (a) predetermined, (b) at the convenience or discretion of the electronic device, and (c) responsive to an external request.

12. The method of claim 9, further comprising repeatedly transmitting the request message via the at least one wireless communication protocol until either reaching a maximum number of transmissions or receiving an acknowledgement (ACK) message.

13. The method of claim 9, wherein the request message comprises at least one of a capture command, a message forwarding command, and identifying information for the central repository.

14. The method of claim 9, wherein the captured information comprises at least one of an image, video, audio, temperature, humidity, location, time, orientation, velocity, and acceleration.

15. The method of claim 9, wherein the at least one peer-to-peer wireless communications protocol comprises at least one of a Long-Term Evolution (LTE) device-to-device (D2D) protocol, an 802.11p protocol, a Bluetooth protocol, and a radio-frequency ID (RFID) protocol.

16. A electronic device, comprising:

a transmitter;

a receiver;

at least one sensor;

a processor; and

at least one memory comprising program code that, when executed by the processor, causes the electronic device to:

receive a request message related to a proximate event via a peer-to-peer wireless communication protocol, wherein the request message comprises an event identification (EID);

capture information related to the proximate event using the at least one sensor; and

transmit a report message comprising the event identification (EID) and at least a portion of the captured information.

17. The electronic device of claim 16, wherein:

the request message related to the proximate event comprises identifying information for a central repository; and

the at least one memory comprises program code that, when executed by the processor, causes the electronic device to transmit the report message to the central repository based on the identifying information.

18. The electronic device of claim 16, wherein:

the at least one memory comprises program code that, when executed by the processor, causes the electronic device to transmit an acknowledgement (ACK) message via a peer-to-peer wireless communication protocol; and

the acknowledgement (ACK) message comprises the event identification (EID).

19. The electronic device of claim 16, wherein:

the request message related to the proximate event comprises a capture command; and

the at least one memory comprises program code that, when executed by the processor, causes the electronic device to capture information related to the proximate event based on the capture command.

20. The electronic device of claim 16, wherein the at least one sensor comprises one or more of a still image camera, a video camera, a microphone, a digital thermometer, a GPS receiver, an accelerometer, a compass, and a gyroscope.

21. The electronic device of claim 16, wherein the peer-to-peer wireless communications protocol comprises one of a Long-Term Evolution (LTE) device-to-device (D2D) protocol, an 802.11p protocol, a Bluetooth protocol, and a radio-frequency ID (RFID) protocol.

22. The electronic device of claim 16, wherein the electronic device is one of a surveillance device and a wireless sensor.

23. An electronic device, comprising:

a transmitter;

a receiver;

at least one sensor;

a processor; and

at least one memory comprising program code that, when executed by the processor, causes the electronic device to:

capture information using the at least one sensor;

determine the occurrence of an event based on the captured information;

associate an event identification (EID) with the captured information;

transmit a request message via at least one peer-to-peer wireless communication protocol, wherein the request message comprises the event identification (EID); and

transmit a report message to a central repository, wherein the report message comprises the event identification (EID) and at least a portion of the captured information.

24. The electronic device of claim 23, wherein the at least one memory comprises program code that, when executed by the processor, causes the electronic device to repeatedly transmit the request message until either reaching a maximum number of transmissions or receiving a minimum number of acknowledgement (ACK) messages.

25. The electronic device of claim 23, wherein the request message comprises at least one of a capture command, a message forwarding command, and identifying information for the central repository.

26. The electronic device of claim 23, wherein the at least one sensor comprises one or more of a still image camera, a video camera, a microphone, a digital thermometer, a GPS receiver, an accelerometer, a compass, and a gyroscope.

27. The electronic device of claim 23, wherein the at least one peer-to-peer wireless communications protocol comprises at least one of a Long-Term Evolution (LTE) device-to-device (D2D) protocol, an 802.11p protocol, a Bluetooth protocol, and a radio-frequency ID (RFID) protocol.

28. The electronic device of claim 23, wherein the electronic device is one of a surveillance device and a wireless sensor.

29. An electronic data collection system, comprising:

a plurality of electronic devices, each comprising a transmitter and a receiver; and

a central repository, comprising a database for storing information, wherein:

the plurality of electronic devices are communicably coupled via a peer-to-peer wireless communication protocol;

the central repository is communicably coupled to the plurality of electronic devices;

at least one of the plurality of electronic devices is operable to transmit a request message directed to the remainder of the plurality of electronic devices, the request message comprising an event identification (EID), a capture command, and identifying information for the central repository;

at least one of the remainder of the plurality of electronic devices is operable to receive the request message, capture information in response to the capture command, and transmit a report message to the central repository, each report message comprising the event identification (EID) and at least a portion of the

information captured by the respective one of the remainder of the plurality of electronic devices; and

the central repository is operable to receive report messages from the plurality of electronic devices, and to store the captured information comprising the report messages in association with the event identification (EID).

30. The electronic data collection system of claim 29, wherein the at least one of the plurality of electronic devices that is operable to transmit a request message is also operable to capture information and to transmit a report message to the central repository comprising the event identification (EID) and at least a portion of the captured information.

31. The electronic data collection system of claim 29, wherein the plurality of electronic devices comprises one of a plurality of surveillance devices and a plurality of nodes in a wireless sensor network.

32. A computer readable medium comprising instructions that, when executed on an electronic device, cause the electronic device to:

receive a request message related to a proximate event via a peer-to-peer wireless communication protocol, wherein the request message comprises an event identification (EID);

capture information related to the proximate event using the at least one sensor; and

transmit a report message comprising the event identification (EID) and at least a portion of the captured information.

33. The computer readable medium of claim 32, further comprising instructions that, when executed by the electronic device, cause the electronic device to transmit the report message to a central repository based on identifying information for the central repository, wherein the request message comprises the identifying information.

34. The computer readable medium of claim 32, further comprising instructions that, when executed by the electronic device, cause the electronic device to transmit the report message substantially contemporaneous with the completion of capturing the at least a portion of the captured information included in the report message.

35. The computer readable medium of claim 32, further comprising instructions that, when executed by the electronic device, cause the electronic device to transmit the report message subsequent to completion of capturing the least a portion of the captured

information included in the report message, at a time that is one of (a) predetermined, (b) at the convenience or discretion of the electronic device, and (c) responsive to a request from the central repository.

36. The computer readable medium of claim 32, further comprising instructions that, when executed by the electronic device, cause the electronic device to transmit the report message in response to an external request.

37. The computer readable medium of claim 32, further comprising instructions that, when executed by the electronic device, cause the electronic device to transmit an acknowledgement (ACK) message via a peer-to-peer wireless communication protocol, wherein the acknowledgement (ACK) message comprises the event identification (EID).

38. The computer readable medium of claim 32, further comprising instructions that, when executed by the electronic device, causes the electronic device to capture information related to the proximate event based on a capture command, wherein the request message related to the proximate event comprises the capture command.

39. The computer readable medium of claim 32, wherein the captured information comprises at least one of an image, video, audio, temperature, humidity, location, time, orientation, velocity, and acceleration.

40. The computer readable medium of claim 32, wherein the peer-to-peer wireless communications protocol comprises one of a Long-Term Evolution (LTE) device-to-device (D2D) protocol, an 802.11p protocol, a Bluetooth protocol, and a radio-frequency ID (RFID) protocol.

41. A computer readable medium comprising instructions that, when executed by an electronic device, cause the electronic device to:

capture information using at least one sensor;

determine the occurrence of an event based on the captured information;

associate an event identification (EID) with the captured information;

transmit a request message via at least one peer-to-peer wireless communication protocol, wherein the request message comprises the event identification (EID); and

transmit a report message to a central repository, wherein the report message comprises the event identification (EID) and at least a portion of the captured information.

42. The computer readable medium of claim 41, further comprising instructions that, when executed by the electronic device, cause the electronic device to transmit the report message substantially contemporaneous with the completion of capturing the at least a portion of the captured information included in the report message.

43. The computer readable medium of claim 41, further comprising instructions that, when executed by the electronic device, cause the electronic device to transmit the report message subsequent to completion of capturing the least a portion of the captured information included in the report message, at a time that is one of (a) predetermined, (b) at the convenience or discretion of the electronic device, and (c) responsive to an external request.

44. The computer readable medium of claim 41, further comprising instructions that, when executed by the electronic device, cause the electronic device to repeatedly transmit the request message until either reaching a maximum number of transmissions or receiving a minimum number of acknowledgement (ACK) messages.

45. The computer readable medium of claim 41, wherein the request message comprises at least one of a capture command, a message forwarding command, and identifying information for the central repository.

46. The computer readable medium of claim 41, wherein the captured information comprises at least one of an image, video, audio, temperature, humidity, location, time, orientation, velocity, and acceleration.

47. The computer readable medium of claim 41, wherein the at least one peer-to-peer wireless communications protocol comprises at least one of a Long-Term Evolution (LTE) device-to-device (D2D) protocol, an 802.11p protocol, a Bluetooth protocol, and a radio-frequency ID (RFID) protocol.

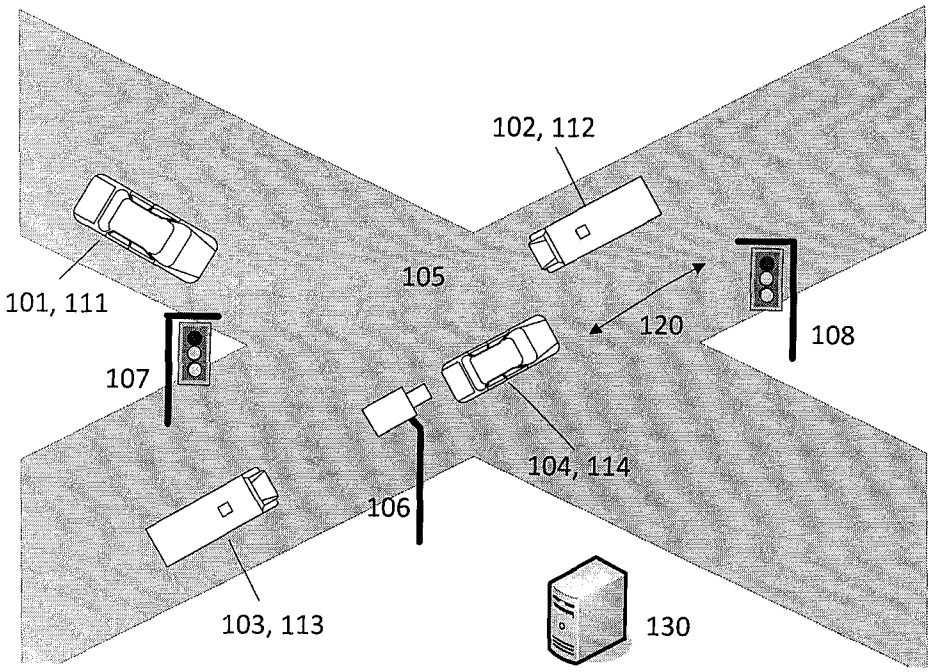

Fig. 1

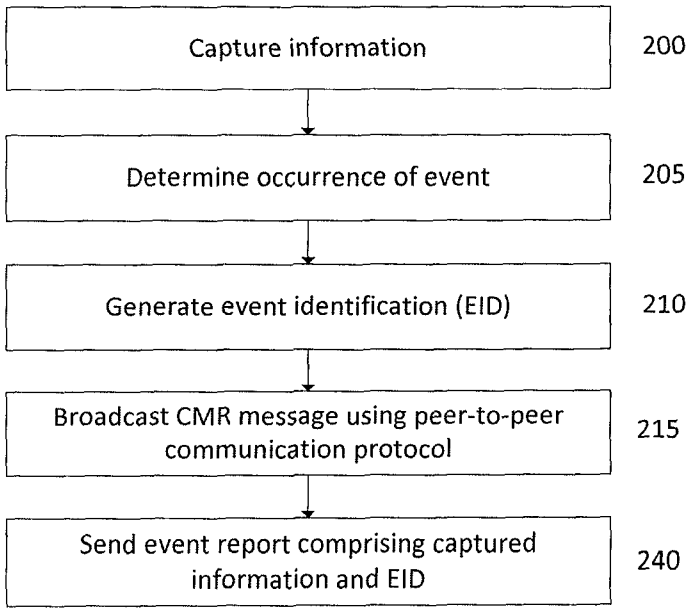
Capture information
200
Determine occurrence of event
205
Generate event identification (EID)
210
Broadcast CMR message using peer-to-peer communication protocol
215
Send event report comprising captured information and EID
240

Fig. 2A

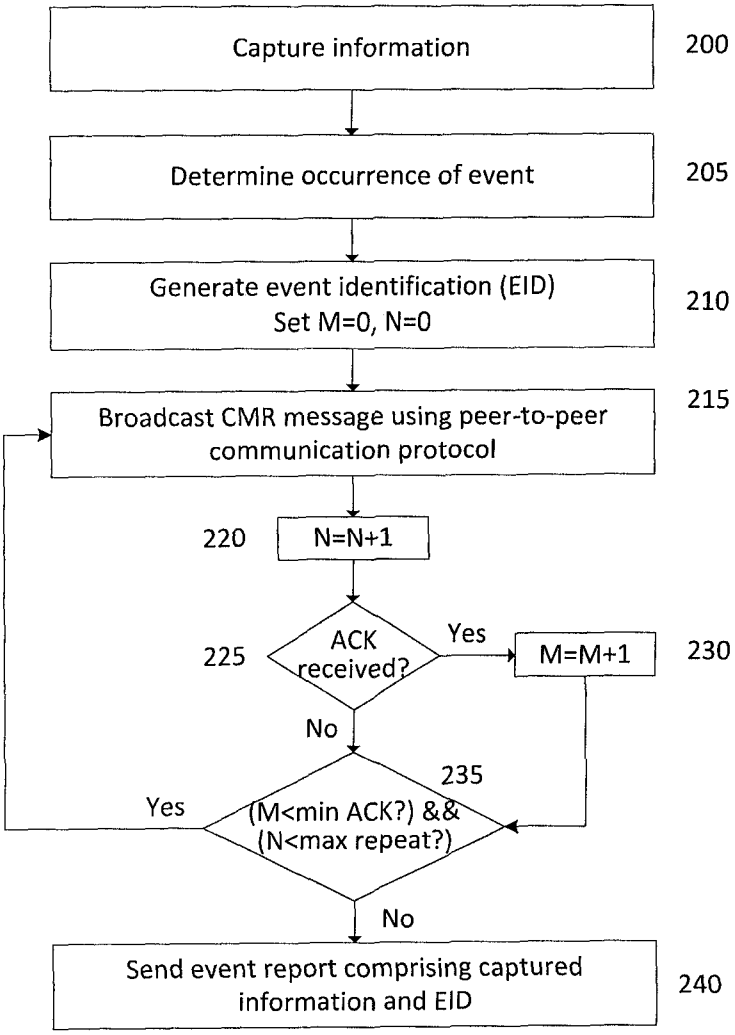
Capture information
200
Determine occurrence of event
205
Generate event identification (EID)
Set M=0, N=0
210
Broadcast CMR message using peer-to-peer communication protocol
215
220
N=N+1
225
ACK received?
Yes
M=M+1
230
No
235
Yes
(M<min ACK?) && (N<max repeat?)
No
Send event report comprising captured information and EID
240

Fig. 2B

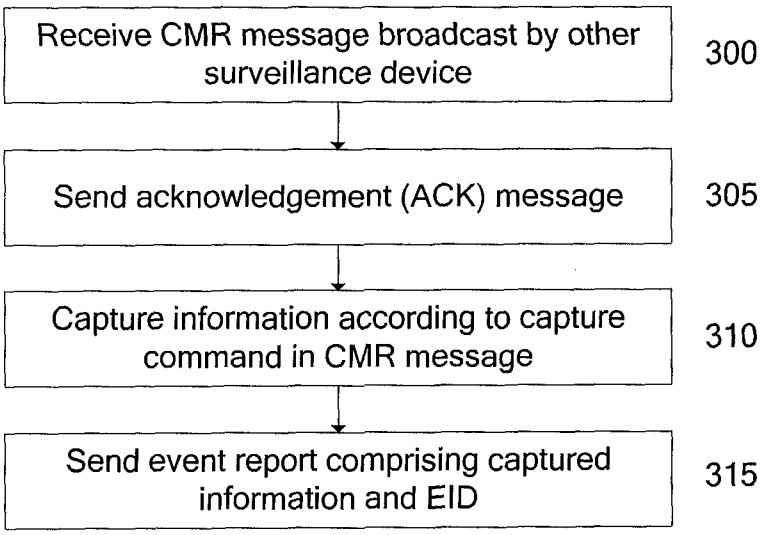
Receive CMR message broadcast by other surveillance device
300
Send acknowledgement (ACK) message
305
Capture information according to capture command in CMR message
310
Send event report comprising captured information and EID
315

Fig. 3

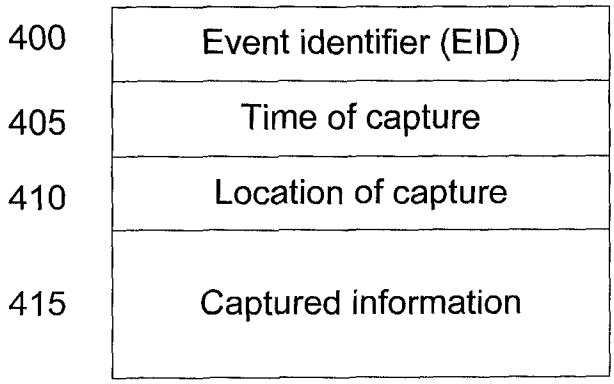
400
Event identifier (EID)
405
Time of capture
410
Location of capture
415
Captured information

Fig. 4A

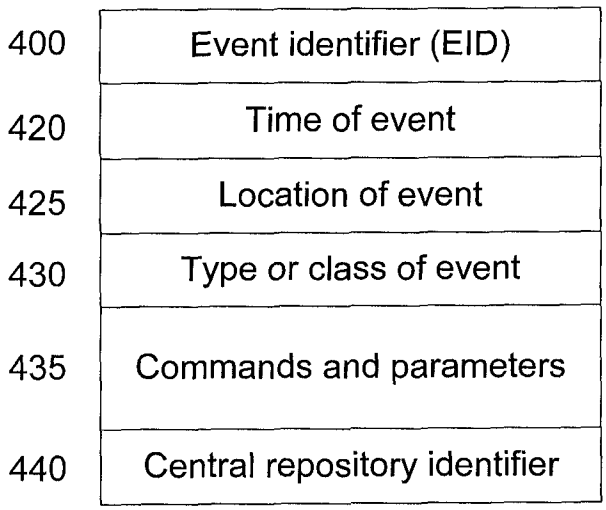
400
Event identifier (EID)
420
Time of event
425
Location of event
430
Type or class of event
435
Commands and parameters
440
Central repository identifier

Fig. 4B

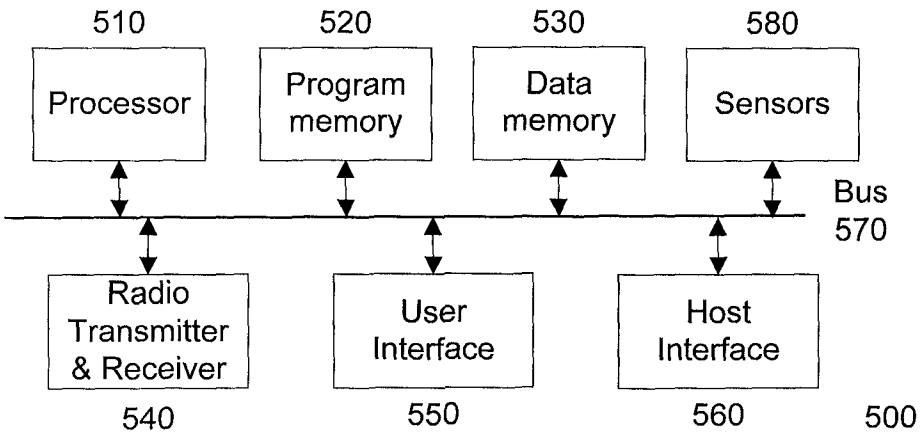
510
520
530
580
Processor
Program memory
Data memory
Sensors
Bus
570
Radio Transmitter & Receiver
User Interface
Host Interface
540
550
560
500

Fig. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2012/077547

A. CLASSIFICATION OF SUBJECT MATTER

H04W 84/18(2009.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04W

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

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

CPRSABS, CNTXT, VEN, USTXT: collection, capture, request, tiger, event, surveillance, sensor, identification, acknowledgement

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN101854653A (UNIV. NANJING POSTS&TELECOM.) 06 Oct. 2010 (06.10.2010)	1-28, 32-47
Y	see the description paragraphs 38-55, figures 1-2	29-31
Y	CN101174356A (UNIV. BEIJING AERONAUTICS&ASTRONAUTICS) 07 May 2008 (07.05.2008) see the description pages 2-4, figures 1-4	29-31
A	CN101052345A (KONINK PHILIPS ELECTRONICS NV) 10 Oct. 2007 (10.10.2007) the whole document	1-47
A	US2006/0139162A1 (HONEYWELL INTERNATIONAL INC.) 29 Jun.29 2006 (29.06.2006) the whole document	1-47

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 Mar. 2013 (25.03.2013)	**04 Apr. 2013 (04.04.2013)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer YU, Hongrui Telephone No. (86-10)62411490

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2012/077547

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US2011/0276440A1 (LYGASE RFID SLOUTIONS) 10 Nov. 2011 (10.11.2011) the whole document	1-47
A	CN102254441A (UNIV. HANGZHOU DIANZI) 23 Nov. 2011 (23.11.2011) the whole document	1-47

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2012/077547

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101854653A	06.10.2010	CN101854653B	15.08.2012
CN101174356A	07.05.2008	CN100507963C	01.07.2009
CN101052345A	10.10.2007	EP1814438B1	17.12.2008
		US2009062626A1	05.03.2009
		EP1814438B8	01.04.2009
		WO2006048840A1	11.05.2006
		IN200702216P4	07.09.2007
		JP5038899B2	03.10.2012
		EP1814438 A1	08.08.2007
		US7924150B2	12.04.2011
		JP2008527466A	24.07.2008
		DE602005011847D1	29.01.2009
		CN100506145C	01.07.2009
US2006/0139162A1	29.06.2009	US7250853B2	31.07.2007
US2011/0276440A1	10.11.2011	NONE	
CN102254441A	23.11.2011	NONE	