



(43) International Publication Date
27 September 2012 (27.09.2012)

- (51) International Patent Classification:
G06F 17/40 (2006.01) *H04W 92/02* (2009.01)
- (21) International Application Number:
PCT/SG2012/000092
- (22) International Filing Date:
21 March 2012 (21.03.2012)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
61/454,872 21 March 2011 (21.03.2011) US
- (71) Applicants (for all designated States except US): **NANYANG TECHNOLOGICAL UNIVERSITY** [SG/SG]; 50 Nanyang Avenue, Singapore 639798 (SG). **SINGAPORE TECHNOLOGIES DYNAMICS PTE LTD** [SG/SG]; 249 Jalan Boon Lay, Singapore 619523 (SG).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **LIM, Hock Beng** [SG/SG]; Nanyang Technological University, c/o Nanyang Innovation & Enterprise Office (NIEO), Blk 1, Unit 213, Innovation Centre, 16 Nanyang Drive, Singapore 637722 (SG). **IQBAL, Mudasser** [PK/SG]; Nanyang Technological University, c/o Nanyang Innovation & Enterprise Office (NIEO), Blk 1, Unit 213, Innovation Centre, 16 Nanyang Drive, Singapore 637722 (SG). **YANG, Daiqin** [CN/SG]; Nanyang Technological University, c/o Nanyang Innovation & Enterprise Office (NIEO), Blk 1, Unit 213, Innovation Centre, 16 Nanyang Drive, Singapore 637722 (SG). **OBAID, Talha** [PK/SG]; Nanyang Technological University, c/o Nanyang Innovation & Enterprise Office (NIEO), Blk 1, Unit 213, Innovation Centre, 16 Nanyang Drive,

Singapore 637722 (SG). **NG, Teng Jie** [SG/SG]; Nanyang Technological University, c/o Nanyang Innovation & Enterprise Office (NIEO), Blk 1, Unit 213, Innovation Centre, 16 Nanyang Drive, Singapore 63772 (SG).

(74) Agent: **VIERING, JENTSCHURA & PARTNER LLP**; P.O. Box 1088, Rochor Post Office, Rochor Road, Singapore 911833 (SG).

(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.

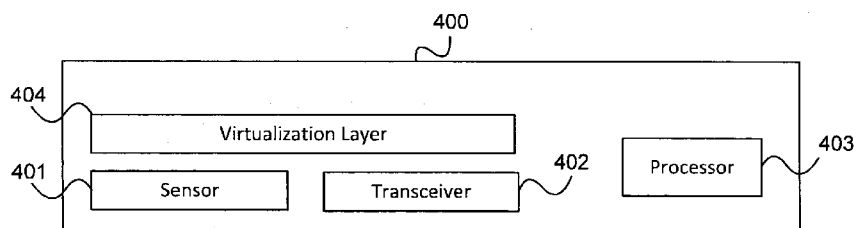
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, 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).

Published:

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

(54) Title: SENSOR DEVICE

FIG 4



(57) Abstract: According to an embodiment, a sensor device is provided comprising a sensor; a transceiver; a processor configured to run an application; and a virtualization layer which comprises an application programming interface encapsulating application layer features of the sensor device and which is configured to provide to the application, via at least one service access point, a service to communicate with another sensor device by means of the transceiver, a service to control the sensor and a service to discover a sensor device network, have the sensor device leave a sensor device network and/or have the sensor device join a sensor device network.



SENSOR DEVICE

Cross-Reference to Related Application

[0001] This application claims priority from United States of America provisional
5 patent application number 61/454,872, filed 21 March 2011, the content of it being
hereby incorporated by reference in its entirety for all purposes.

Technical Field

[0002] Various embodiments relate to a sensor device.

10

Background

[0003] The rapid advances and convergence of technologies such as MEMS (Micro
Electro-Mechanical Systems) sensor devices, wireless networks and low-power
embedded processors have enabled a new generation of large-scale wireless sensor
15 networks (WSN). In the near future, tiny and cheap sensors may be extensively
embedded within our living environment for sensing a large variety of physical
phenomena of interest to users. Unlike information services on the Internet where the
information often becomes stale or even useless, sensor networks can seamlessly
couple the physical environment with the digital world and deliver useful real-time
20 information to users according to their needs.

[0004] Wireless sensor networks have attracted tremendous interest in the industry
because they have many important applications including environmental monitoring,
healthcare, industrial automation, military and homeland security, disaster warning
and rescue, manufacturing and logistics, intelligent transportation, safety monitoring

of urban and civil infrastructures, smart grid, smart buildings and homes, and many other applications that we do not yet imagine.

[0005] These enormous business prospects spurred investments in the development of sensor network platform technologies at both the hardware and software operating platform level. At the hardware level, the sensor nodes offer a mix of sensing, processing, communication and storage capabilities. Some commonly used sensor node platforms include the MicaZ, iMote2, IRIS, TelosB, Atmel Raven, Gumstix and Sentilla JCreate from vendors such as Memsic, Atmel, Gumstix and Sentilla.

[0006] However, these hardware platforms differ in the processor specifications, storage file system, communication protocols and sensor technologies. At the operating and programming platform level, these sensor node platforms are based on different platforms such as TinyOS, Contiki, .Net Micro Framework, embedded Linux, Sentilla, etc. In addition, the wireless communication protocols also vary from platform to platform and there exists a plethora of different protocols that are supported by various vendors. Some common wireless networking protocols for sensor networks include IEEE 802.15.4, ZigBee, TinyOS MAC, 6LoWPAN, SICSLoWPAN, and GSM/3G.

Summary

[0007] Various embodiments provide a sensor device comprising a sensor; a transceiver; a processor configured to run an application; and a virtualization layer which comprises an application programming interface encapsulating application layer features of the sensor device and which is configured to provide to the application, via at least one service access point, a service to communicate with another sensor device by means of the transceiver, a service to control the sensor and

a service to discover a sensor device network, have the sensor device leave a sensor device network and/or have the sensor device join a sensor device network.

Brief Description of the Drawings

5 [0008] In the drawings, like reference characters generally refer to like parts throughout the different views. The drawings are not necessarily to scale, emphasis instead generally being placed upon illustrating the principles of some example embodiments of the invention. In the following description, various example embodiments of the invention are described with reference to the following drawings,
10 in which:

Figure 1 shows a sensor device network (also referred to as sensor network) according to an embodiment.

Figure 2 shows two sensor devices.

Figure 3 shows two sensor devices.

15 Figure 4 shows two a sensor device according to an embodiment.

Figure 5 shows two sensor devices according to an embodiment.

Figure 6 shows a virtualization layer according to an embodiment.

Figure 7 shows two sensor devices according to an embodiment.

20 Figure 8 illustrates the components of a runtime environment according to an embodiment.

Figure 9 illustrates the components of an API according to an embodiment.

Detailed Description

[0009] The following detailed description refers to the accompanying drawings that
25 show, by way of illustration, specific details and embodiments in which the invention

may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention. Other embodiments may be utilized and structural, logical, and electrical changes may be made without departing from the scope of the invention. The various embodiments are not necessarily mutually
5 exclusive, as some embodiments can be combined with one or more other embodiments to form new embodiments.

[0010] Figure 1 shows a sensor device network (also referred to as sensor network) 100 according to an embodiment.

[0011] The sensor device network 100 includes a plurality of sensor devices 101, 102,
10 103, in this example a first sensor device 101, a second sensor device 102 and a third sensor device 103.

[0012] The sensor devices 101, 102, 103 may communicate via communication connections 104, 105, 106, in this example a first communication connection 104 between the first sensor device 101 and the second sensor device 102, a second
15 communication connection 105 between the first sensor device 101 and the third sensor device 103 and a third communication connection 106 between the second sensor device 102 and the third sensor device 103.

[0013] The topology of the sensor device network 100 may for example be a single hop star where all the sensor devices 101, 102, 103 are within transmission range of
20 each other and multiple sensor nodes respond to a command node (or central controller; not shown).

[0014] The communication via the communication connections 104, 105, 106 may be carried out according to various communication protocols and may include wireless or wireline communication. For example, the communication may be carried out
25 according to one or more of the wireless networking protocols IEEE 802.15.4,

ZigBee, TinyOS MAC, 6LoWPAN, SICSLowPAN, and GSM/3G. Different sensor devices 101, 102, 103 may support different communication protocols.

[0015] At the hardware level, the sensor devices (also referred to as sensor nodes or just nodes) 101, 102, 103 may provide functions for sensing, processing,

5 communication and data storage. For this, they may for example include one or more sensor modules, one or more actuators, a processor and one or more memories. The sensor devices 101, 102, 103 may for example be configured according to one or more of the sensor node platforms MicaZ, iMote2, IRIS, TelosB, Atmel Raven, Gumstix and Sentilla JCreate from vendors such as Memsic, Atmel, Gumstix and
10 Sentilla.

[0016] At the operating and programming platform level, these sensor node platforms are for example based on different platforms such as TinyOS, Contiki, .Net Micro Framework, embedded Linux, Sentilla, etc.

[0017] Different sensor devices 101, 102, 103 may be based on different platforms
15 (and for example use different operating systems).

[0018] Heterogeneity in sensor networks can be categorized into four dimensions: hardware platform, operating system, communication stack, and application schema.

The hardware platform of a sensor node defines its physical attributes including sensor modules, communication modules, embedded processors and memories. There
20 are many commercially available hardware platforms, including MicaZ, IRIS, iMote2, TelosB, SunSpot, Gumstix, etc., which differ from each other in terms of processor feature, memory capacity, I/O interface, etc. Heterogeneity in hardware platforms results in different low-level processing mechanism, part of which can be encapsulated by the operating system and shielded from programmers. To facilitate
25 the development of sensor network applications, there are several event-driven

programming model with their tailored extensions of the C programming language.

TinyOS applications are constructed through defining static wiring structure among modularized software components while Contiki C uses protothreads to support multitasking. Both of them provide a rich component library.

- 5 [0019] Apart from the hardware/software platform differences of sensor nodes, when networked sensor applications are concerned, two more heterogeneity dimensions are introduced. The first heterogeneity is the networking protocol heterogeneity. As sensor networks are usually constrained by the processing, memory, and energy limitations of sensor nodes, many application tailored networking protocols have been
- 10 proposed to cope with such constraints and improve system performance. With different networking protocols, it is very difficult to integrate sensor network systems and make them interoperable. The second heterogeneity lies in the application layer which handles data and service management. Interoperable sensor nodes should share the same knowledge about how to make use of the data and other functionalities (aka
- 15 services) provided by other sensor nodes.

[0020] The following items may be seen as the two main factors that affect the operation of a sensor network:

[0021] a. Application Programmability

- [0022] Sensor nodes 101, 102, 103 using different hardware/software platforms may
- 20 be programmed over incoherent platforms and programming interfaces which form the corresponding application layer. This includes the operating environments used such as TinyOS, Contiki, embedded Linux, etc. Each sensor node 101, 102, 103 may provide different features in a unique manner. In addition, programmability also covers the different functionalities of the sensor network 100 such as joining a

network, requesting and providing data, commanding different sensor nodes 101, 102, 103 to carry out sensing tasks, etc.

[0023] This is illustrated in figure 2.

[0024] Figure 2 shows two sensor devices 201, 202.

5 [0025] In this example, each sensor device 201, 202 runs a respective application 203, 204, supports a respective network protocol 205, 206, runs a respective operating system 207, 208 and is based on a respective hardware platform 209, 210.

[0026] Figure 2 conceptually illustrates that two sensor nodes (or sensor networks in case that the sensor nodes belong to different sensor networks) 201, 202 cannot
10 interoperate due to having heterogeneous application layers (i.e. different applications 203, 204, e.g. different applications for controlling the operating of the respective sensor device 201, 202). Even if the two sensor nodes 201, 202 have similar lower layers (e.g. if the network protocols 205, 206 are equal, the operating systems 207, 208 are equal and the hardware platforms 209, 210 are equal), they may be unable to
15 make use of the data and other functionalities (i.e. services) provided by each other if they do not speak the same language (i.e. use a different programming model, data management, etc.). Thus, there may be difficulties in discovering what sensor nodes are available in two sensor networks, what their capabilities are, what services they offer, and how to make use of their services.

20 [0027] b. Interconnecting Network Protocol

[0028] At the network layer, different protocols may specify the packet formats, traffic management, the network topologies of the sensor node networks, etc.

[0029] This is illustrated in figure 3.

[0030] Figure 3 shows two sensor devices 301, 302.

[0031] In this example, each sensor device 301, 302 runs a respective application 303, 304, supports a respective network protocol 305, 306, runs a respective operating system 307, 308 and is based on a respective hardware platform 309, 310.

[0032] Figure 3 conceptually shows the lack of interoperability due to heterogeneous network layers 305, 306. If the two sensor nodes 301, 302 (or two sensor networks in case that the two sensor nodes 301, 302 are of different sensor networks) use the same application layer, they may still remain "invisible" to each other since they cannot interpret the network traffic from each other, and thus cannot be involved in in-network data processing.

[0033] Thus, sensor nodes 101, 102, 103 with heterogeneous application layers and/or network layers may not be able to interoperate, and it may thus be very difficult to build a large-scale sensor network 100 using sensor nodes 101, 102, 103 of different platforms (e.g. using different operating systems, network protocols, etc.). Indeed, most sensor network deployments make use of sensor nodes of similar platforms. In practice, a large-scale sensor network (such as a sensor network for environmental monitoring) is typically developed and deployed in several phases. A small-scale prototype sensor network is first deployed to experiment with those basic sensing-actuation tasks that are fundamental to the application. In the later phases, this sensor network is then enhanced to handle more complicated sensing tasks, employ better wireless networking technologies or harness the processing/storage power of new sensor node platforms. To build and deploy a powerful but yet cost-efficient large-scale sensor network, it typically makes sense to use sensor nodes that provide the best combination of functionalities and value for money. Also, due to the phased deployment strategy, it is impractical to replace the entire sensor network with the latest sensor node platforms, given the investment already made for the existing

sensor network. In fact, it is often impractical to replace a sensor node with another node once it has been deployed in the field. Thus, the existing restriction of having to deploy similar sensor nodes in a network may greatly limit the scalability and flexibility in terms of managing the ongoing cost of deploying and upgrading sensor networks using different, cheaper and advanced sensor nodes.

[0034] These heterogeneity challenges may for example be addressed by unifying the respective layers. For example, IBM's Mote Runner and Sentilla's JCreate introduce a virtual machine in a node to support programming in multiple languages for the same platform. However, in order to achieve interoperability of heterogeneous platforms, the respective virtual machine on each platform is needed and thus the original interoperability problem may be seen to persist.

[0035] For the application layer, approaches such as OpenWSN and ZigBee introduce a very application specific application layer that can only be used in a specific application such as utility services or control and automation. These different application layers cannot be extended to build other sensor network applications and they do not interoperate as well.

[0036] Likewise, devices and solutions that enable interoperability between different network layer protocols such as 6LoWPAN and ZigBee allow interoperability only in a peer-to-peer single hop setting and do not provide interoperability between two Wireless Personal Area Networks (WPANs). Co-existing WPANs can use the same radio interface with different protocol suites. For example, Zigbee, 6LoWPAN, WirelessHART and other IEEE 802.15.4 protocol based WPANs share the same wireless radio with each other. The radios of co-existing WPANs may also be different. For example, a WPAN may be Bluetooth based while the other may be UWB based.

[0037] Virtualization may be introduced into sensor networks in various ways.

Examples include the following:

- a. Create virtual sensors to compensate for the lack of physical sensors or to produce high-level processed data using low-level data from physical sensors.
- 5 b. Develop virtual programming environments that can generate platform-specific codes based on high-level logic.

[0038] However, these approaches require a unique software layer (operating system and application) to be used in place of the existing very rich operating platforms.

They are not able to make use of the features and capabilities that are already
10 available in the existing platforms and thus can be seen to not really solve the issue of interoperability. They also require programmers to be trained for programming in the new platform and thus the existing code-base is wasted.

[0039] According to one embodiment, a virtualization technology is used which addresses enabling heterogeneous layers to co-exist in the same sensor network or
15 interoperate while in different sensor networks. One embodiment builds on top of existing platforms (e.g. hardware platforms) so that not only their features can be reused, but existing applications and code-base can also be integrated and reused. The virtualization framework according to various embodiments pushes the application limits of sensor networks by overcoming the existing limitation of using sensor nodes
20 of a similar platform in a network.

[0040] In other words, according to one embodiment, the issue of heterogeneity of sensor devices is addressed by a semantics-based and service-oriented virtualization framework to handle the heterogeneities and enable transparent interoperability. The underlying philosophy of the virtualization framework according to an embodiment
25 can be seen in changing the way applications are developed by introducing a

virtualization layer between the operating system and sensor network applications.

This, according to one embodiment, is illustrated in figure 4.

[0041] Figure 4 shows a sensor device 400 according to an embodiment.

[0042] The sensor device 400 comprises a sensor 401, a transceiver 402 and a
5 processor 403 configured to run an application.

[0043] The sensor device 400 further comprises a virtualization layer 404 which
comprises an application programming interface encapsulating application layer
features of the sensor device and which is configured to provide to the application, via
at least one service access point, a service to communicate with another sensor device
10 by means of the transceiver, a service to control the sensor and a service to at least
one of discover a sensor device network, have the sensor device leave a sensor device
network and have the sensor device join a sensor device network.

[0044] According to one embodiment, in other words, a virtualization layer
encapsulates the functionalities of a sensor device (such as communication and sensor
15 control) such that they are accessible, e.g. via a predetermined interface, i.e.
predetermined service access points, by an application.

[0045] According to one embodiment, the processor is further configured to run an
operating system and the virtualization layer is above the operating system layer.

[0046] According to one embodiment, the processor is further configured to run an
20 operating system implementing a network protocol stack and the virtualization layer
is configured to provide the service to communicate with another sensor device by
means of the network protocol stack.

[0047] The virtualization layer may encapsulate the network protocol stack.

[0048] According to one embodiment, the service to control the sensor includes
25 controlling the sensor to perform a sensing operation.

[0049] According to one embodiment, the virtualization layer comprises a runtime environment.

[0050] According to one embodiment, the sensor device comprises a hardware platform including the sensor and the transceiver. The hardware platform is for example MicaZ, iMote2, IRIS, TelosB, Atmel Raven, Gumstix or Sentilla JCreate but is not limited to these.

[0051] According to one embodiment, the service to communicate with another sensor device is a service to communication with another sensor device having a different hardware platform.

10 [0052] According to one embodiment, the virtualization layer provides routing functionality.

[0053] According to one embodiment, the virtualization layer provides network protocol translation functionality.

15 [0054] According to one embodiment, the processor is further configured to run a TinyOS, Contiki, .Net Micro Framework, embedded Linux or Sentilla operating system.

[0055] According to one embodiment, the processor is further configured to run an operating system and the service to communicate with another sensor device is a service to communication with another sensor device running a different operating system.

20 [0056] According to one embodiment, the virtualization layer is implemented by means of the processor.

[0057] Two sensor device including a virtualization layer according to an embodiment are illustrated in figure 5.

25 [0058] Figure 5 shows two sensor devices 501, 502.

[0059] In this example, each sensor device 501, 502 runs a respective application 503, 504, respective operating system 507, 508 and is based on a respective hardware platform 509, 510. Further, each sensor device 501, 502 includes a respective virtualization layer 505, 506.

5 [0060] The virtualization layer 505, 506 of each sensor device 501, 502 includes a runtime environment and an application programming interface (API) as it is illustrated in figure 6.

[0061] Figure 6 shows a virtualization layer 600 according to an embodiment.

[0062] The virtualization layer 600 includes a runtime environment 601 and an API
10 602 which will be described in more detail below.

[0063] The virtualization layer 505, 506 of each sensor device 501, 502 includes four components, namely an API 511, 512, an application schema 513, 514, a protocol management component 515, 516 and a hardware abstraction component 517, 518.

[0064] On the application programming level, the application schema 513, 514, also
15 referred to as Generalized Application Schema (GAS), and the Application Programming Interface (API) allow, through flexible configurations of those functions, accommodation of diversified applications. According to one embodiment, the design of this schema has three merits: 1) it is general enough to cover the requirements of diversified applications; 2) it provides over-the-air configurability
20 such that the application can be easily configured and retrofitted; 3) it does not rely on central servers and control functions can be distributed into the system to reduce system traffic load and shorten event response time. The schema may be designed on top of a general sensor (and actuator) network and deals with the application layer of the protocol stack. According to one embodiment, under-layer protocols such as the
25 physical layer, media access control (MAC) layer and network layer protocols are

outside the scope of this schema. Adopting this approach in the application layer of each sensing and actuation device can help to shift the workload from pre-deployment system design to post-deployment application design. The time required for system development can be shortened and the deployment procedure can be simplified.

- 5 Furthermore, the schema can also be used as a shared application interface in heterogeneous sensor and actuator networks to support both interoperability and scalability.

[0065] The application schema 513, 514 included in the virtualization layer 505, 506 provides a unified and generalized sensor network application schema. It enables
10 integration and interoperability among distributed and heterogeneous sensor nodes and can serve as a unified application interface to integrate distributed applications through the Service-Oriented Architecture (SOA) approach. The API 511, 512 of the virtualization framework 505, 506 encapsulates the application schema 513, 514 into programming interfaces as well as provides functions for easy manipulation of
15 underlying networking protocols. With this API 511, 512 diversified sensor network applications conforming to the same application schema can be easily developed.

[0066] According to one embodiment, separate versions of the runtime 601 and the API 602 (e.g. of an API library) of the virtualization layer 505, 506 are built on top of different sensor network operating systems 507, 508 which may for example include
20 TinyOS and Contiki. Building multiple versions of the virtualization layer 505, 506 on top of several popular operating systems enables interoperability among heterogeneous operating systems and also preserves the advantages of the large code-base and user community of these established operating systems. Programmers can stick to their familiar operating systems and enjoy a smooth learning curve of the
25 transition phase towards virtualization.

[0067] The protocol management component 515, 516 takes care of protocol abstraction and encapsulation when the sensor node 501, 502 interconnects with other sensor nodes through networking protocols and enables interconnectivity between different networking protocols. Arbitrary stripped down versions of networking protocol suites may be supported by the protocol management component 515, 516 to cope with the energy limitations of the sensor nodes 501, 502.

[0068] The hardware abstraction component 517, 518 of the virtualization framework sits on top of the existing operating system 507, 508 and interacts directly with the underlying platform's hardware resources, i.e. the hardware platform 509, 510. It may for example enable transparent access to the underlying hardware resources from other sensor nodes with different operating systems.

[0069] Regarding the network level interoperability, connecting all sensor nodes or sensor networks to the Internet is a simple way to address interconnection issues. As long as all sensor networks (e.g. WPANs) are connected to the Internet, they can communicate with each other. However, as the Internet does not manage locality information of each WPAN. Even if co-existing WPANs can communicate with each other through the Internet, it is very difficult for them to discover their co-location status and cooperate on location-based issues.

[0070] On the contrary, local interconnectivity among co-existing WPANs not only provides connectivity but also helps to better exploit and share knowledge locally among the vicinity such that Location Based Services (LBS), which can be seen as crucial part of Ambient Intelligence technologies, could be greatly facilitated. With the usage of a virtualization layer according to various embodiments, local cooperation can be supported across different (device level) radio technologies and (system level) WPAN deployments. Further, a convenient way for instant data sharing

among proximate devices without the support of other infrastructure based systems, such as the Internet, is provided.

[0071] With the current trend of connecting WPANs to the Internet, there are many corresponding efforts to decouple the applications of existing WPANs from their under-layer protocols and transplant them onto Internet protocol suites, such as the adaptation of ZigBee Application Layer (ZAL) over UDP. With the virtualization according to various embodiments, these decoupled applications can be directly adopted by embedded devices, despite their under-layer protocols. Designs of new applications of embedded devices can also be totally protocol transparent.

[0072] According to one embodiment, the virtualization framework provides the following features:

- Encapsulation of the network protocol stack in an Application Programming Interface (API) such that the programmers can develop intelligent techniques to dynamically switch between the various network layers and thus seamlessly connect to a multitude of personal and wide area networks.
- Encapsulation of connectivity mechanisms such as WiFi, 3G, 6LoWPAN, ZigBee, etc.
- Encapsulation and unification of application schema for sensing, actuation and control that supports wider range of application development for sensor networks.
- Service-oriented mechanisms for discovering, joining, operating and leaving a sensor network with heterogeneous nodes.

[0073] Further features and effects of the virtualization framework according to various embodiments may include the following:

- It changes the way sensor networks and other embedded devices are programmed. It provides an API that encapsulates the application layer features provided by each platform and develops unified application programming interfaces. Thus, programmers on different platforms need not re-think their application design for each different platform, and they can reuse the higher level application logic across the most common spectrum of sensor network application layers.
- It allows reuse of already existing application code where a large amount of valuable man hours have already been spent.
- It exploits the platform-specific application layer features, yet it allows interoperability between heterogeneous platforms via unified application interfaces.
- It encapsulates the interconnectivity between the nodes and the networks and provides programming interfaces to make the nodes and networks intelligently switch between the network protocols.
- By providing functions to build application and network gateways, it allows interoperability between heterogeneous wide and personal area networks.
- Scalable design in terms of being able to accommodate new platform that may be available in the future.

[0074] Various embodiments can be seen to leverage the concepts of platform virtualization (PV), service-oriented architecture (SOA), and semantic web (SW) to address the incoherency between communication standards and data interpretation.

[0075] Platform Virtualization: Virtualization technologies may include operating system virtualization, storage virtualization, network virtualization, memory virtualization, I/O virtualization, application virtualization, desktop virtualization, etc.

The concept of platform virtualization can be seen in developing an intermediate layer between the hardware resources and the operating platform such that any operating platform can be used on any underlying hardware.

[0076] Service-Oriented Architecture: The importance of SOA in enterprise computing

5 is widely recognized. SOA is a software architecture to enable loosely coupled integration and interoperability of distributed heterogeneous systems by using services as component elements. Services are computational entities that can be described, published, discovered, orchestrated and invoked by other software entities. An SOA usually includes directory services that service providers register with. A
10 request for a service with desired characteristics often results in a matchmaking process based on the profiles stored in the directory. Even if no adequate services are found in this manner, it is still possible to build composite services by combining several existing services.

[0077] Semantic Web: Semantics is the solution for finding meaningful information

15 and integrating with the related information. This semantic provenance imposes a formally defined domain- specific conceptual view on sensor data, mitigates or eliminates terminological heterogeneity, and enables the use of reasoning tools for knowledge discovery. Ontology is the key technology behind semantics for making information more meaningful by adding more knowledge. The term ontology can be
20 defined as an explicit formal specification of concepts. Ontology binds together classes or concepts that may have subclasses to represent more specific concepts than in super-classes, properties or relationships that describe various features and properties of the concepts, also termed as slots that are superimposed on the defined classes and/or properties to define allowed values (domain and range).

[0078] As illustrated in figure 5, the operation of the sensor nodes 501, 502 is categorized into different layers. The hardware platform layer 509, 510 of a sensor node 501, 502 specifies the physical attributes of the sensor node 501, 502 such as the sensor modules (e.g. one or more sensors), communication modules, the embedded processor and the memory. The next layer is the operating system layer 507, 508 that defines the firmware/middleware programming environment. The operating system layer 507, 508 exposes the capabilities of the sensor node 501, 502 (sensing, routing, storage, etc.) based on the underlying hardware platform 509, 510. The operating system may support a particular network layer and the application (or a plurality of applications) 503, 504 may be built on top of the operating system.

[0079] Thus, the manner in which the underlying platform is utilized by an application is largely defined by the operating system; how different nodes talk to each other is defined by the network layer; and how various nodes in the network implement and understand the application logic is defined by the application layer.

[0080] The virtualization layer 505, 506 allows two sensor nodes 501, 502 having different network and application layers with different mechanisms for data logging, data representation, data processing, and routing to interoperate.

[0081] According to one embodiment, the virtualization layer 505, 506 that sits on top of the operating system 507, 508 of a sensor device 501, 502 encapsulates the network layer and the application layer of the sensor device. This added layer functions on top of the operating system (also referred to as the host operating system) and provides the ability to use different application and network layers while making use of the system-level features provided by the operating system. This is illustrated in figure 7.

[0082] Figure 7 shows two sensor devices 701, 702.

[0083] In this example, each sensor device 701, 702 runs a respective application 703, 704, has a respective virtualization layer 705, 706, runs a respective operating system 707, 708 and is based on a respective hardware platform 309, 310.

[0084] The virtualization layer 705, 706 of a sensor device 701, 702 supports various
5 network protocols (e.g. a first network protocol 711 and a second network protocol 712) and applications (e.g. a first application 713 and a second application 714), and enables the programmers to develop applications 703, 704 on top of the virtualization layer. Thus, it is possible to exploit any network and application layer available within the virtualization layer 705, 706.

10 [0085] This design also allows making the application 503, 504 independent from the network protocols 711, 712. Thus, the application developer can simultaneously use traditionally incompatible network layers and application layers such as ZigBee on the application layer with 6LoWPAN on the network layer. In addition, he can also develop application and network layer gateways between two sensor networks or
15 sensor devices running different network layer protocols and application layer protocols. Such gateways can perform the translation on the network layer and application layer and enable transparent interoperability between heterogeneous devices.

[0086] According to one embodiment, the overall design of the virtualization layer is
20 based on the SOA such that the capabilities of the sensor nodes 701, 702 are exposed and used as services including the network layer and the application layer.

[0087] The runtime environment 601 (see figure 6) is for example a small footprint of the virtualization layer 600 that hosts core services to handle on-node jobs and network interconnectivity whereas the API 602 provides a unified mechanism for

developing the programmer and application specific services that are also managed by the runtime environment 601 in a unified manner.

[0088] The components of the runtime environment 601 according to an embodiment are illustrated in figure 8.

5 [0089] Figure 8 illustrates the components of a runtime environment 800 according to an embodiment.

[0090] The runtime environment 800 (or virtualization layer runtime) comprises generic services 801, network management 802, service management 803, and tables 804, 805, 806 to keep track of jobs, routes and services. These runtime services either
10 stay active all the time or are invoked on-demand to handle various tasks. A packet parser 808 of the generic services 801 receives all the in-bound packets and parses them to identify whether the packet should be routed or should be consumed by the node itself. For routing, the network management service route discovery 814 and the routing table 805 are utilized. If the packet is to be consumed by the sensor node itself,
15 then an auto reply service 809 is invoked if the packet requests something from the sensor node that can be served by the services that are part of the node's runtime. For example, if the packet is for a service discovery, then a discovery service 816 in the service management 803 tier is invoked, and the details of the services hosted on the sensor node are retrieved from the service table 806 (which may for example include
20 application semantics 807) and an automatic reply is sent back to the requesting party.

[0091] If the incoming packet requests for a sensing, actuation or automation control task to be initiated on the node, then the scheduling 810, execution control 811 and job table 804 components are used to schedule this task for execution.

[0092] The network management 802 components of the runtime also include a
25 protocol translation service 815 that can dynamically switch from one protocol to the

other. This component implements various network layer protocol stacks such as IEEE 802.15.4, TinyOS MAC, ZigBee and IPv6-based 6LoWPAN. Essentially, this component encapsulates various network layer protocols at the application layer and thus allows interoperability between heterogeneous network layers in a node-to-node or a node-to-network fashion. Initialization 812, maintenance 813 and route discovery 814 components of the network management 802 may also be employed for setting up the network layer, maintaining the routes and routing the traffic, respectively.

[0093] The virtualization layer runtime 800 also includes core components to manage the services on the node as part of the service management 803 functionalities. These include service discovery 816, invocation 817 and termination 818 components that are invoked automatically in response to requests. The service table 806 is maintained to serve as a registry for service configurations that can be dynamically retrofitted by a dynamic configuration component 813. The SOA approach provides application level interoperability between heterogeneous application layers and enables the building of a application/service translation component 820. This component makes use of the Application Semantics 807 for various application layers and allows programmers to translate to and fro between various applications.

[0094] The components of the API 602 according to an embodiment are illustrated in figure 9.

[0095] Figure 9 illustrates the components of an API 900 according to an embodiment.

[0096] According to one embodiment, the virtualization layer API 900 builds on top of the native operating system and encapsulates application services, network protocols, node level and data management features to expose them as functions to the application programmers. The various components of the API 900 and their sub-

components are shown in figure 9. The purpose of the API 900 is to enable application programmers to build sensor network applications in a unified manner by explicitly or implicitly using various application and network layers encapsulated within the API 900. The programmers develop application logic and the services specific to the application, and the deployment on the node will be handled by the virtualization layer's runtime core services. For example, the API 900 is implemented for the most common sensor network platforms that support C, Java and NesC languages. The libraries in the API belong to four main classes: service management 901, network management 902, node management 903 and data management 904.

[0097] Service management libraries 901 enable programmers to interface with the sensors and actuation hardware available on the node using a sensing interface 905 and an actuation interface 906. Through a create service library 907 and a utilize service library 908, the programmers can build complex workflows and deploy them on the nodes. An automation control library 909 provides a protocol-based approach for creating and activating complex control tasks, such as gathering data from a number of sensors, processing the data and reporting to the sink node in case of a significant event. Such automation controls are built on top of the existing core sensing and actuation services on the nodes. The service management 901 also allows starting and stopping services 910 and the building of the application logic to remotely discover services on known and unknown nodes 911 and over known and unknown protocols 912, thus enabling true interoperability.

[0098] The network management libraries 902 provide basic features such as discovering 912, joining 913 and leaving a sensor network 914. A switch network protocol interface 915 and a network protocol interface 916 are used in case of joining and operating in heterogeneous network layers. A convenient network diagnostics

library 917 provides functions to detect anomalies in the network such as disconnections, bandwidth, throughput, etc. from the application layer's perspective.

[0099] Since the health of the node itself is also crucial and its semantics should also be configured for network visibility purposes and to design the application logic, the node management 903 provides a node semantics configuration library 918 and a node diagnostics library 919. The semantics management allows access to parameters such as the node's identification, visibility role, time sources, physical and logical location, network address, etc. The diagnostics that can be accessed include the node's battery, memory and CPU status, permanent storage, etc.

[00100] The data management library 904 can be seen as an important feature of the API 900 that provides basic data management and processing functions. These include a data sink function 920 to gather data from a node or the network to another location, data sync 921 between one or more nodes in the network, data compression 922 to conserve network bandwidth and data security 923 to preserve data privacy and allow authenticated access.

[00101] It should be noted that the API features can be used in a cascaded manner such that data can be gathered in a particular application layer context and processed in a different application and transmitted over a different network protocol. This feature allows truly scalable interoperability ease of programming over heterogeneous sensor network platforms.

[00102] The operating system is for example an RTOS (Real Time Operating System). In such an operating system, threads are termed tasks and can be scheduled individually through specifying priority and having delays within tasks. Similar to Contiki, a continuous service is needed to run a task. Inter-thread communication and

coordination is achieved through RTOS primitives like mutexes, semaphores, events, mailboxes and timers. This is illustrated in figure 10.

[00103] Figure 10 shows a task diagram 1000.

[00104] In the task diagram 1000, arrows 1001 represent possible calls to tasks

5 1002 including a control manager task, an app task, a parser task, a receive task and a send task. Every task 1002 other than the receive task has a mailbox which acts like a notification queue. Every send of an element into the queue notifies the task 1002.

There is a mutex controlling the using of the radio resource shared by both the receive task and the send task.

10 [00105] The task functionalities are as described above, e.g. may include functionalities of the runtime 800 described with reference to figure 8. According to one embodiment, the control manager task handles creation, deletion and servicing of the automations by keeping a registry 1003 of similar content as the sensing manager which has been implemented. Each automation might be serviced by an individual
15 timer. These control services can be passive or active. The control manager task also services control service discovery. The app (application) task resolves decisions made by application layer, such as receiving of data or service discovery report.

[00106] In the following, examples for control service packets are given.

[00107] A Control Auto Enabling Packet (with homogenous input and single
20 output) may for example have the following format:

01001xxx	8 bits	8 bits	8 bits		
Frame	Destination	Time	Method ID	Input List	Output List
control	Auto ID	window			

[00108] The following flags may be included (e.g. in the frame control field):

f1: homogeneous input?

f2: Src type of input sensing data (given f1 is ON)

1. Control auto
2. Sensing device

f3: output type

- 5 1. Sensing data
2. Actuation command

[00109] The input list may for example have the following format.

8 bits		16 bits	8 bits	
Number of input	Input src type (f1 OFF)	Src address of input 1	Src service ID/ Auto ID 1	...

[00110] The output list may for example have the following format:

8 bits	8 bits
Destination address of output	Destination service ID/ Auto

[00111] According to one embodiment, a Sensing Data Report Packet as follows is

10 used:

10101xxx	8 bits	8 bits	
Frame control	Destination Auto ID	Source Service ID/ Auto ID	Data
			Value Time

[00112] The following flags may be included (e.g. in the frame control field):

f1: ack – request

f2: auto – enabled

f3: Source service type, sensing service or control automation

- 15 [00113] It should be noted that the broad application spectrum of sensor networks is well established. The deployment of large-scale sensor networks involves stakeholders such as government agencies, industrial companies, research institutions

and system integrators. Sensor network applications have provided substantial benefits and cost savings through their remote surveillance, actuation and alert mechanisms. Thus the spectrum of sensor network applications is ever expanding and there is increased attention to seek higher returns on investment by reducing on-going
5 infrastructural operational, repair and upgrade costs.

[00114] The sensor network virtualization technology according to various embodiments can be applied in a broad spectrum of application domains such as environmental monitoring, homeland security, battlefield operations, disaster warning and rescue, industrial automation, healthcare monitoring, transportation, smart
10 buildings, smart grids, etc. Potential customers include sensor network technology providers and technology integrators. The technology integrators will indirectly represent their clients such as government agencies and large companies which require heterogeneous sensor network solutions. The demand for interoperable sensor network technologies from technology integrators may motivate sensor network
15 technology providers to include support for a virtualization framework as provided according to various embodiments as a built-in feature of their platforms. Likewise, the ability to develop interoperable sensor networks may be necessary for many applications, thus promoting the adoption of a virtualization framework.

[00115] Sensor network platform providers may find greater interest in the
20 technology according to various embodiments as it pushes the limits to which sensor networks can be applied. These providers may find it indispensable to provide the virtualization framework according to various embodiments as part of their product offerings due to the expected growing user interest.

[00116] Thus, as the sensor network market grows, the sensor network virtualization technology according to embodiments may find even greater clientele due to the flexibility and cost-value benefit it offers to customers.

[00117] While the invention has been particularly shown and described with
5 reference to specific example embodiments, it should be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the invention as defined by the appended claims. The scope of the invention is thus indicated by the appended claims and all changes which come within the meaning and range of equivalency of the claims are
10 therefore intended to be embraced.

CLAIMS

1. A sensor device comprising

a sensor;

a transceiver;

5 a processor configured to run an application; and

a virtualization layer which comprises an application programming interface

encapsulating application layer features of the sensor device and which is

configured to provide to the application, via at least one service access point, a

service to communicate with another sensor device by means of the

10 transceiver, a service to control the sensor and a service to discover a sensor

device network, have the sensor device leave a sensor device network and/or

have the sensor device join a sensor device network.

2. The sensor device according to claim 1, wherein the processor is further

15 configured to run an operating system and the virtualization layer is above the

operating system layer.

3. The sensor device according to claim 1, wherein the processor is further

configured to run an operating system implementing a network protocol stack

20 and the virtualization layer is configured to provide the service to

communicate with another sensor device by means of the network protocol

stack.

4. The sensor device according to claim 3, wherein the virtualization layer

25 encapsulates the network protocol stack.

5. The sensor device according to claim 1, wherein the service to control the sensor includes controlling the sensor to perform a sensing operation.

5 6. The sensor device according to claim 1, wherein the virtualization layer comprises a runtime environment.

7. The sensor device according to claim 1, comprising a hardware platform including the sensor and the transceiver.

10

8. The sensor device according to claim 7, wherein the hardware platform is MicaZ, iMote2, IRIS, TelosB, Atmel Raven, Gumstix or Sentilla JCreate.

9. The sensor device according to claim 1, wherein the service to communicate with another sensor device is a service to communication with another sensor device having a different hardware platform.

15

10. The sensor device according to claim 1, wherein the virtualization layer provides routing functionality.

20

11. The sensor device according to claim 1, wherein the virtualization layer provides network protocol translation functionality.

12. The sensor device according to claim 1, wherein the processor is further configured to run a TinyOS, Contiki, .Net Micro Framework, embedded Linux or Sentilla operating system.
- 5 13. The sensor device according to claim 1, the processor is further configured to run an operating system and wherein the service to communicate with another sensor device is a service to communication with another sensor device running a different operating system.
- 10 14. The sensor device according to claim 1, wherein the virtualization layer is implemented by means of the processor.

100

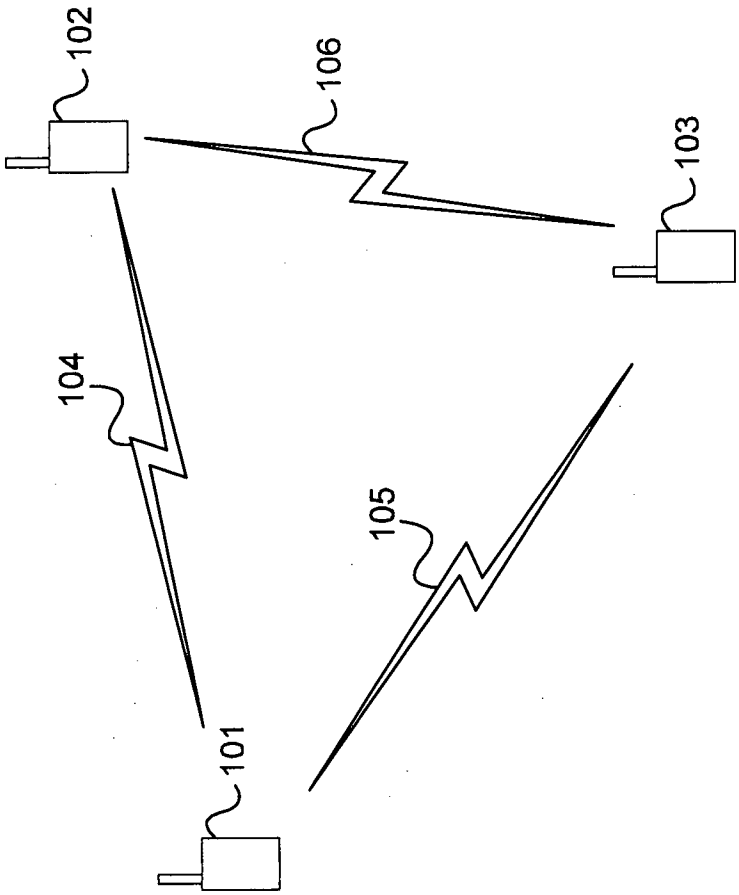


FIG 1

FIG 2

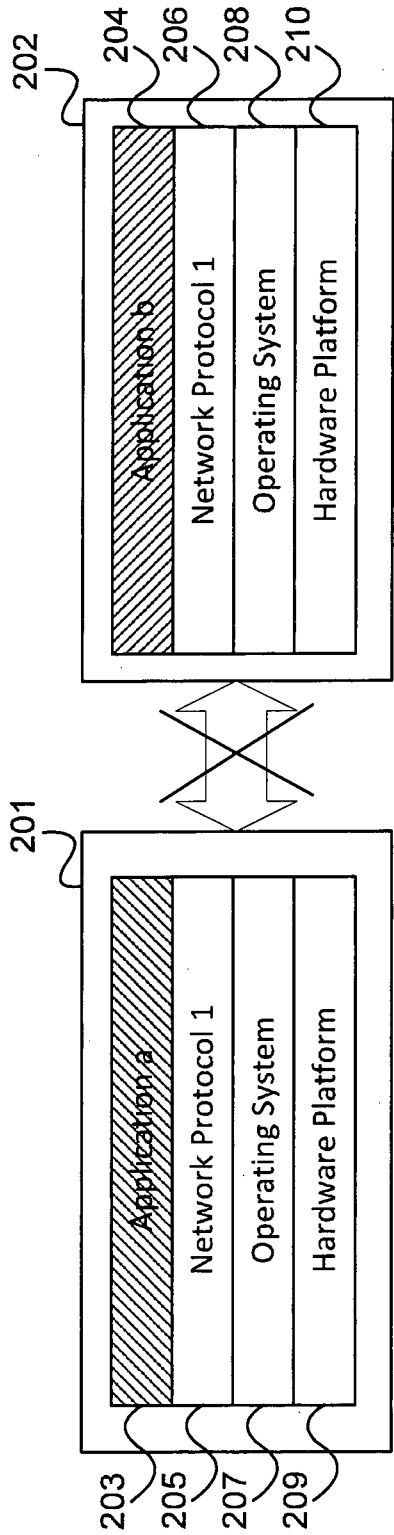


FIG 3

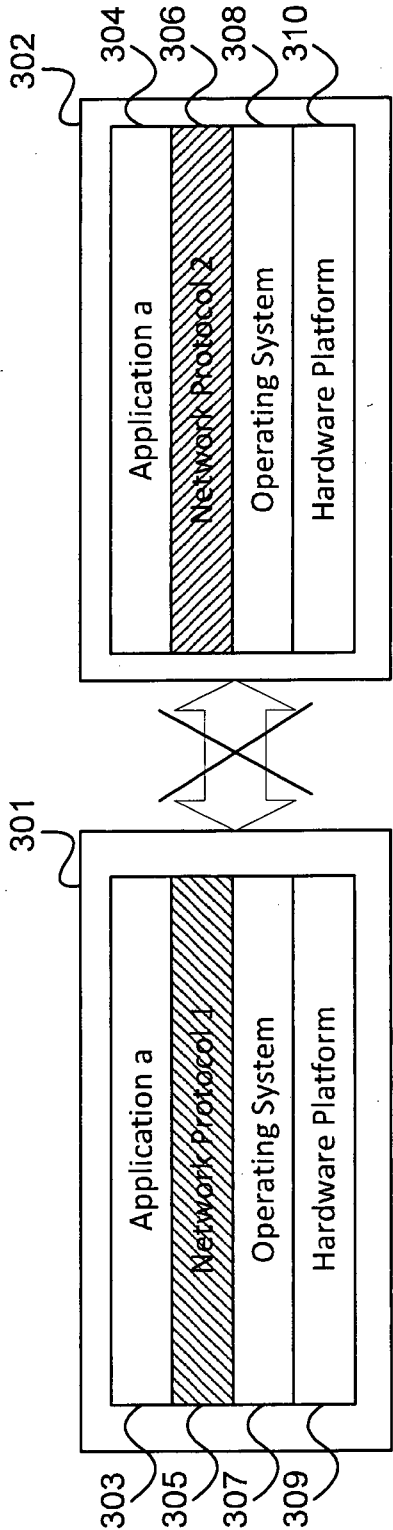


FIG 4

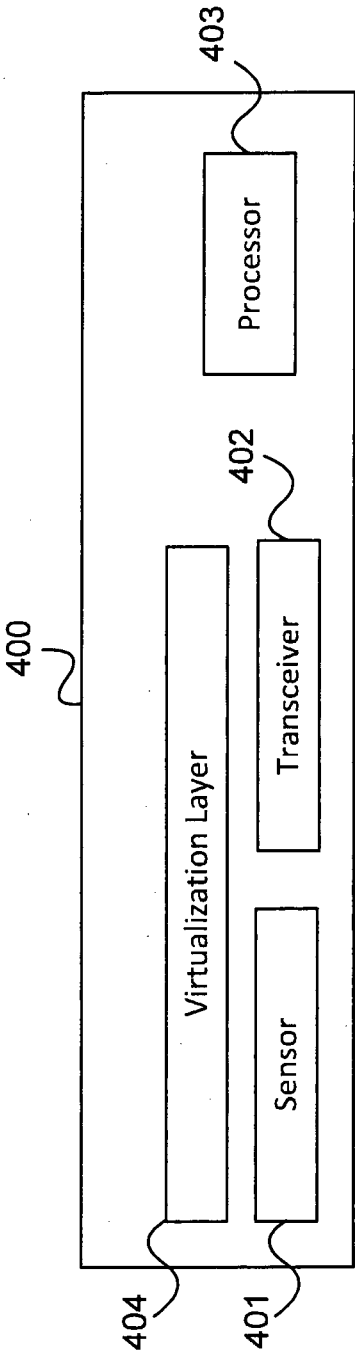
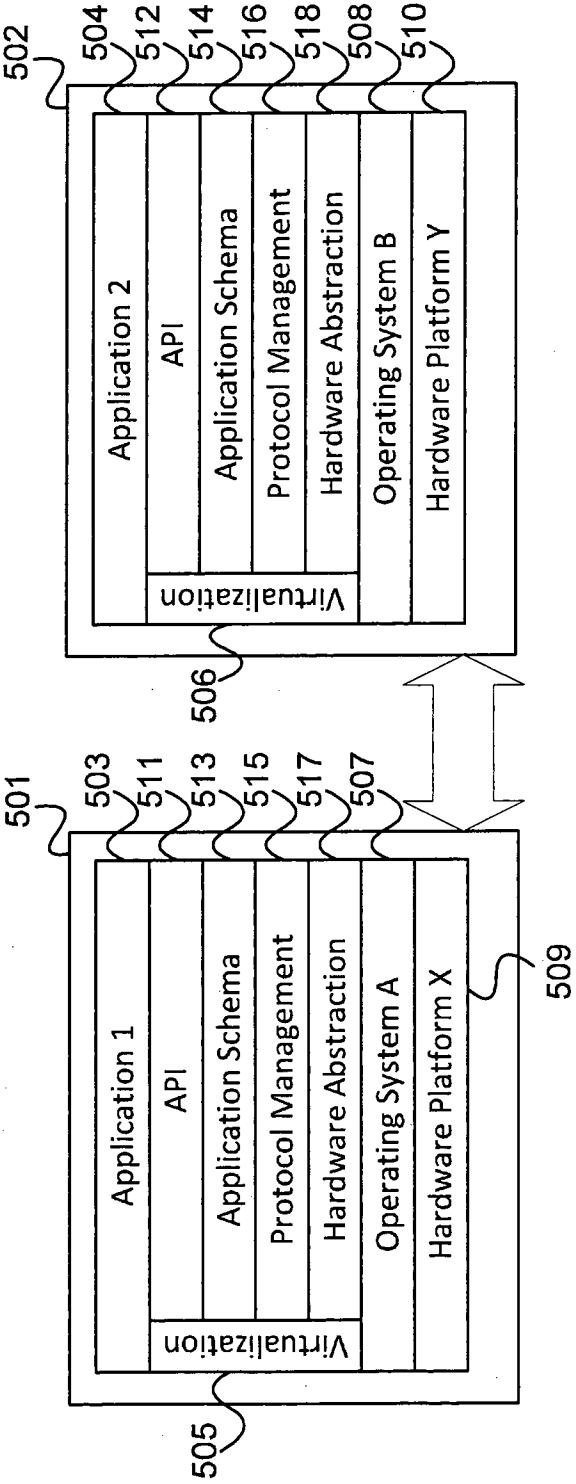


FIG 5



600

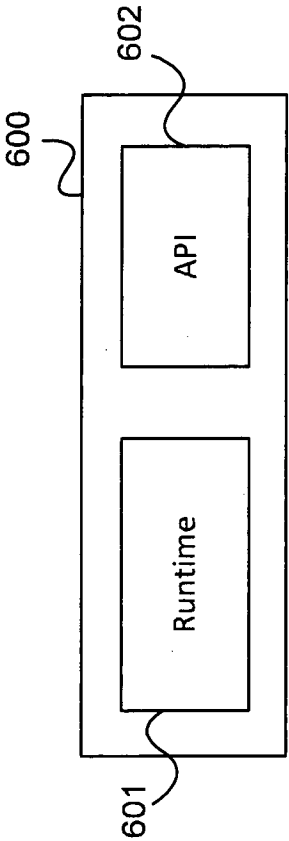
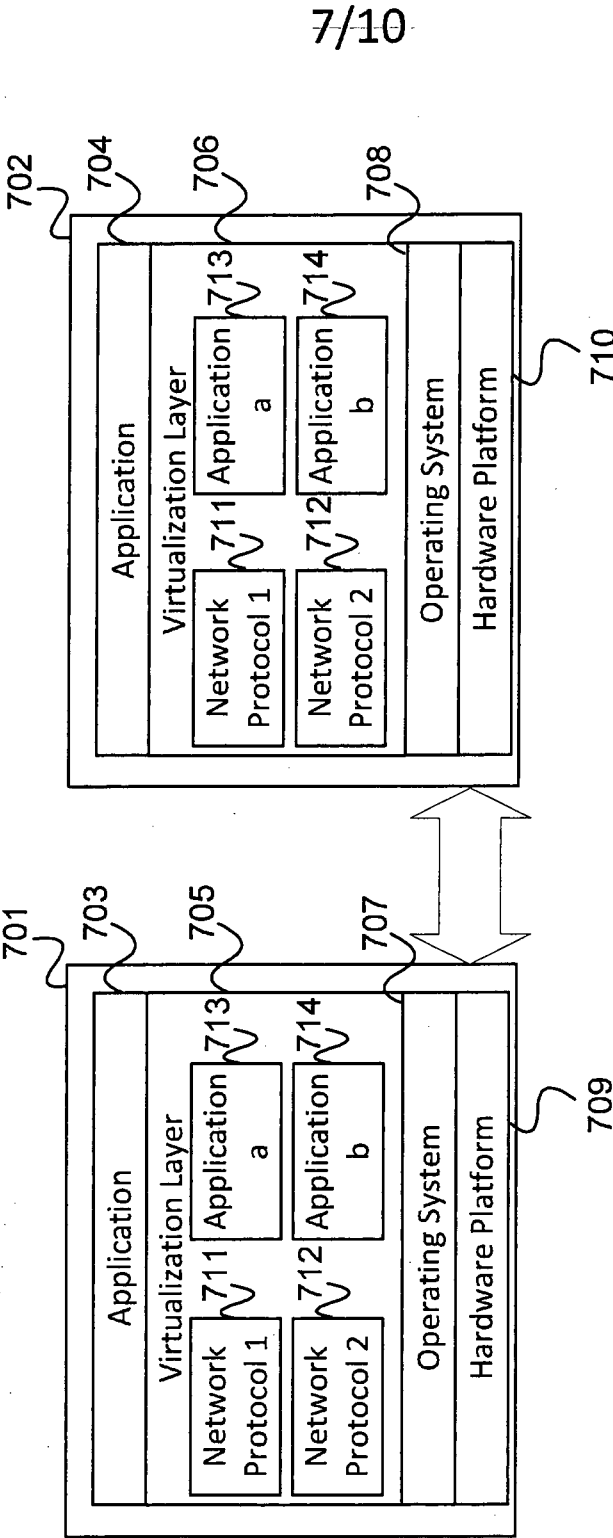
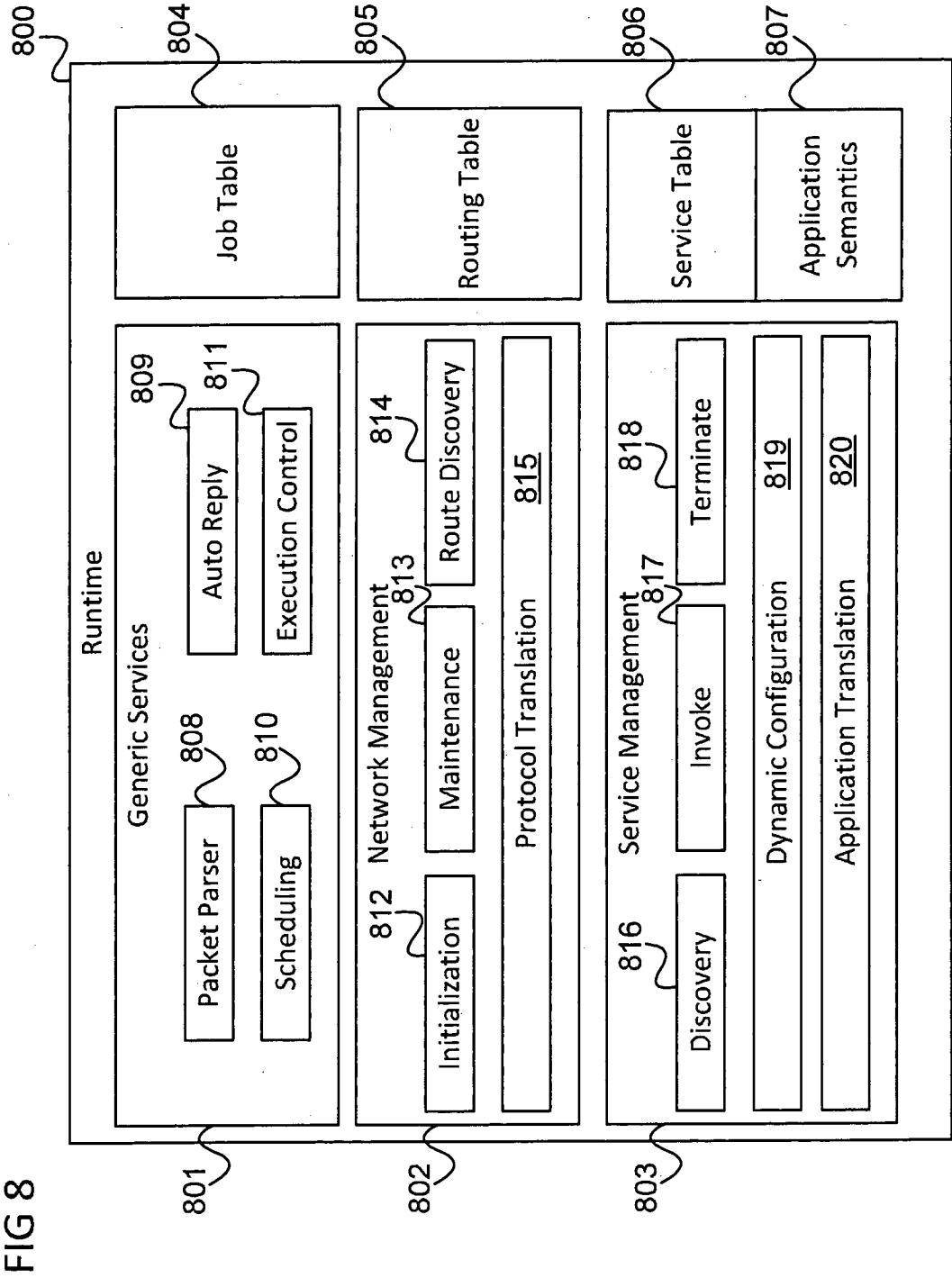


FIG 6

FIG 7





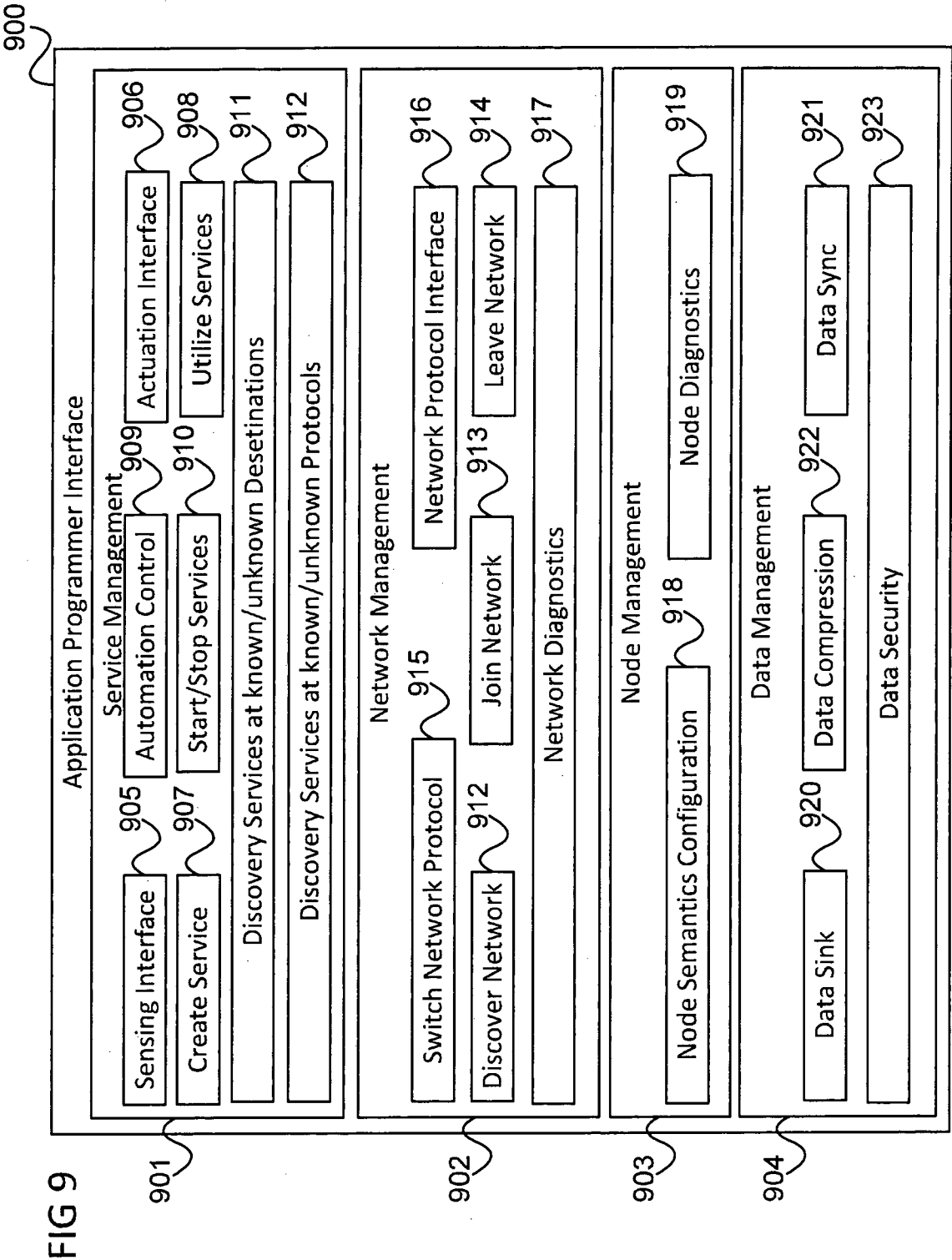
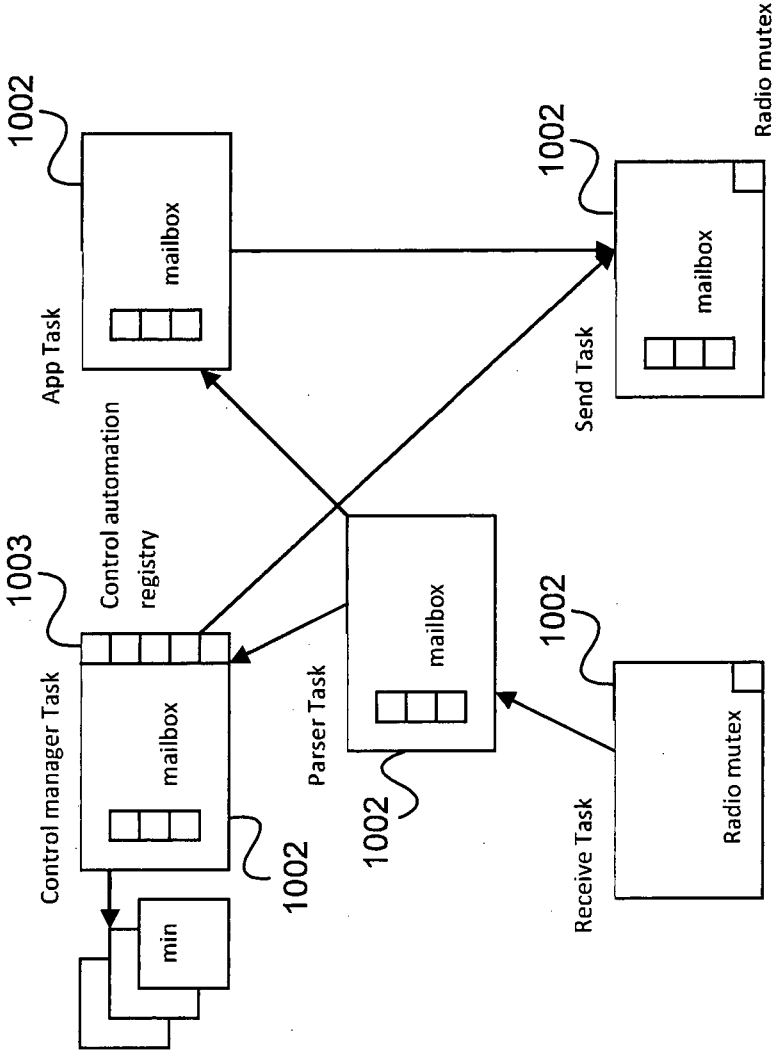


FIG 10

1000



INTERNATIONAL SEARCH REPORT

International application No.

PCT/SG2012/000092

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

G06F 17/40 (2006.01)

H04W 92/02 (2009.01)

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)

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)

Patent Lens, WPI, EPODOC (sensor, network, virtual etc...)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/0098594 A1 (GANESH) 11 May 2006 Figures 2, 6 and 16, Paragraphs [0010], [0034], [0051]-[0053], [0059], [0181], [0208], [0210]	1-14

☐ 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	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"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
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

30 May 2012

Date of mailing of the international search report

5 June 2012

Name and mailing address of the ISA/AU

AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
E-mail address: pct@ipaustalia.gov.au
Facsimile No. +61 2 6283 7999

Authorized officer

ANDREW ELLETT
AUSTRALIAN PATENT OFFICE
(ISO 9001 Quality Certified Service)
Telephone No : +61 2 6225 6120

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/SG2012/000092

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member	
US	2006098594	US	7561544
Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.			
END OF ANNEX			