

Distributed Federated Sensor Network

Ran Xu

Department of Computer Science
Loughborough University
Loughborough, U.K.
r.xu@lboro.ac.uk

Shuang-Hua Yang

Department of Computer Science
Loughborough University
Loughborough, U.K.
s.h.yang@lboro.ac.uk

***Abstract-** Wireless sensor networks have been used increasingly widely in the modern world. The sensor nodes in the network system not only have a small physical size, but also have low energy consumption albeit with low processing ability. Wireless sensor networks are used to collect data in remote or harsh conditions, which in reality requires a number of different heterogeneous sensor network. There are a number of challenges here such as determining the equipment and services to use, the data query methods, the methods for network connection, as well as numerous security issues. In fact, how to collect data from multiple sensor networks subject to the user's requirement is becoming a most critical problem. In this paper, we present a demonstration for a data centralized Federated Sensor Network. Our demonstration shows that the centralized architecture is not a perfect solution for on-demand sensor data. Therefore, we introduce a novel distributed Federated Sensor Network architecture. A comparison between centralized and distributed architectures for Federated Sensor Networks is given at the end of the paper to inform any possible implementation.*

Keywords: Collaborative, Federated Sensor Network, Centralized, Distributed, Comparison.

1 Introduction

Wireless sensor networks (WSN) are more and more seen as the solution to large-scale tracking and monitoring applications. It is a self-organizing network composed of random distributing nodes, which include build-in sensors, a data processing unit and a communication module. It uses build-in sensors to detect phenomena such as temperature, humidity, infrared radiation, and sonar and radar signals. Such types of sensors can provide useful information for a wide variety of purposes [1]. The communication method used can be wired, wireless, infrared or light, but it is generally agreed that short-range low power wireless communication is most suitable for sensor network [2]. The deployment and management of these networks, however, is usually handled by a single controlling entity (i.e., owner). Furthermore, a sensor network is often dedicated to a single application. This is due to the fact that we do not yet have the means to deal with a secure multi-purpose federated sensor network,

involving hundreds of different applications requiring the same sensor data from one sensor network at the same time, or one application asking sensor data from thousands of different types of sensor network. Depending on the query load, the priority and urgency of each application, sensing, bandwidth and computation resources must be carefully allocated to provide desirable quality-of-service, whilst preserving fairness, security of operation and privacy across applications.

With the popularity of wireless sensor network, several applications have been developed by civilian and business as well as by military users [3]. As a consequence of the nature of WSN, each network is independent from all others, which means that the data collected by one WSN can only be analyzed and used by a single application. This feature limits the availability and usability of such sensor data. In addition, sensor data is often meaningless unless it is associated with other data such as time, position etc. Unfortunately, existing designs do not consider the situation where several WSNs work together. Therefore, a system, which combines multiple sensor networks for collaborative working, is required. We call such collaboration a Federated Sensor Network.

So far, there are two types of query methods, which are widely used in various kinds of networks. The first one is centralized data queries. It is similar to the processes of accessing a warehouse. The data are extracted from the sensor networks in a predefined way and stored in a centralized database system that is responsible for query processing [4]. This approach is well suited for aggregate queries over historical data, but not so good for querying real-time sensor data obtained directly from the sensor networks, because it is too expensive to transmit a continuous sensor data flow. It is also a significant waste of resources to extract data from the whole sensor network to satisfy a single query. An alternative query method is decentralized query [5], in which the data is uploaded only when necessary, the application, which generates the query, can contact the data source directly to extract data. This approach is desirable for live data transmission but cannot return history data because the individual sensor network has no connected database. It also leads to a huge waste of network resources when numerous queries are referencing the same data source. So a new approach,

which combined the advantages of both Centralized query and decentralized query, is needed.

2 Related work and problems

Most of the related work uses a central database to collect all the sensor data and then transmit it to the requesting applications. An example is the SenseWeb [6] from Microsoft Research, which aims to provide a common platform and set of tools to enable MSN Live data owners to easily publish their sensor data. The SenseWeb platform transparently provides mechanisms to archive and index data, process queries and to aggregate and present the results on a geo-centric web interfaces such as MSN Virtual Earth, etc. It collects data from sensors (which could be cameras, thermometers, theatre booking computers etc), which may be either placed permanently at some locations or located in a moving vehicle. The sensor data will be pushed to a central database for indexing after which it becomes available for being queried. Then the online mapping system provides particular information from which a user could select a location [7]. The system is accessible to general Microsoft LIVE users as a mean of presenting the results of searching sensor data. Its deficiencies include all the defects of a centralized data collection. In addition, the SenseWeb is working as a data monitoring system. Thus the user can only get sensor data from the Central Database, and is not able to directly access the sensor network.

3 Centralized Federated Sensor Network

For the Federated Sensor Network project a provisional system architecture has been published [8]. It contains four components with an optional part for implementing large scale networks. As shown in *Figure 1*:

- a) A Data Node: is an extra node in a WSN, which collect sensor data and transfers it to a system host or the system backup database. The data collection node can join the WSN automatically without any modification to the current sensor network. When the host cannot obtain a connection directly from a sensor network, In order to ensure that the sensor data reaches the central database safely, the sensor data will be transferred by passing it through this node, as it is not part of the sensor network.
- b) Sensor Gateway: this can connect with different types of sensor network. The system architecture has been built using all of the above components. This appears to be a promising method to make WSNs connect and work collaborative.
- c) Virtual Coordinator: this monitors and controls the central database directly and provides the user with the analyzed result of the sensor data.
- d) Applications: these are the data consumers that present the output to the user and the system administrator via the management terminal.

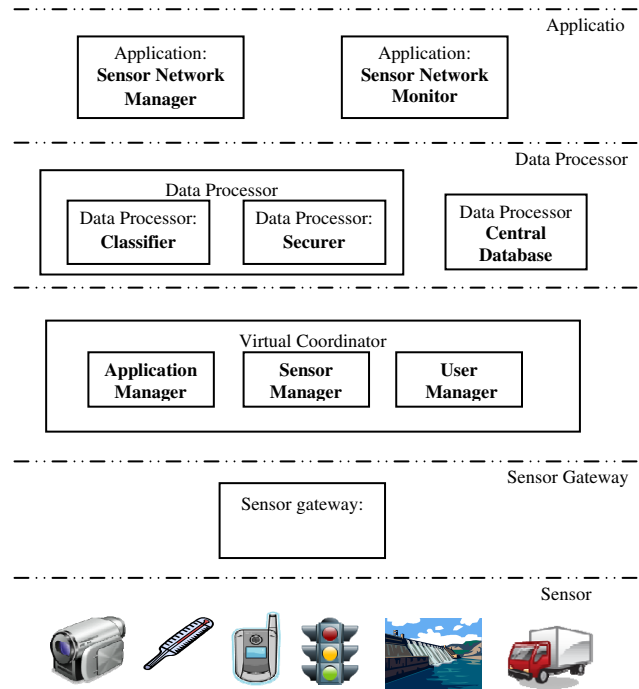


Figure 1. The system architecture of a centralized FSN

Indeed, the entire system is based on a centralized structure. As such it is optimal at indexing and searching historical sensor data, but weak on querying live data. A simple model of a Sensor Gateway and Data Node has been developed using JAVA. Because a ZigBee sensor network is used as the sensor source, the Data Node needs to have a serial port connection. The communication protocol between the Data Node and the Sensor Gateway is TCP/IP, as shown in *figure 2*. There is a PC connected to each Zigbee network as a Data Node. The Data Node (client), using Internet access, can connect with the Sensor Gateway (server). In the Sensor Gateway, the operator needs to open a port to start listening for incoming connection requests. When there is a new client request for connection, the Sensor Gateway will create a new thread and open a new port for receiving the data.

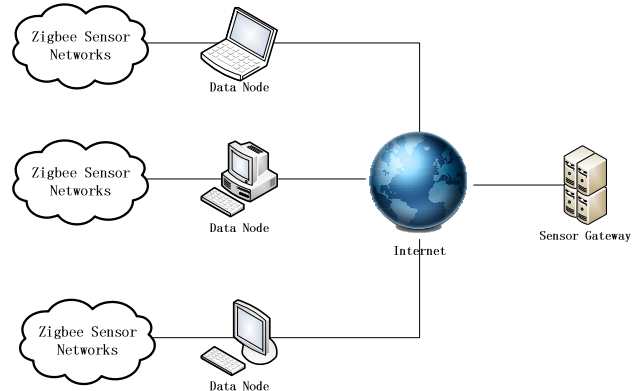


Figure 2. Demonstration architecture

Once the Data Node has been set up, the sensor data sent out by the ZigBee networks will be recorded, this includes

continuous sensor data flow and exceptional condition report for the sensing environment. The sensor data will be forwarded to the Sensor Gateway (server) with a predetermined IP address and listening port number. As shown on *figure 3*.

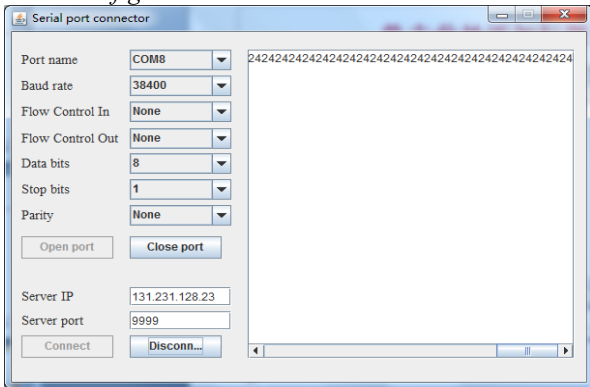


Figure 3. Sensor Node application

The listening port of the Sensor Gateway is for receiving connection request from Data Nodes. It will open a new window and a new port and then create a new thread to receive and display the sensor data. The connection will be dropped if the operator presses the disconnect button or closes the window (see *Figure 4*)

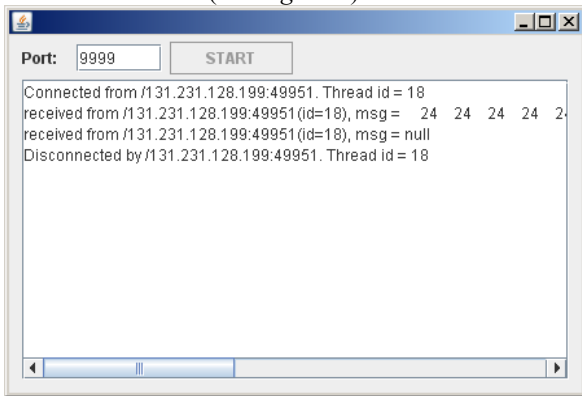


Figure 4. Sensor Gateway main window

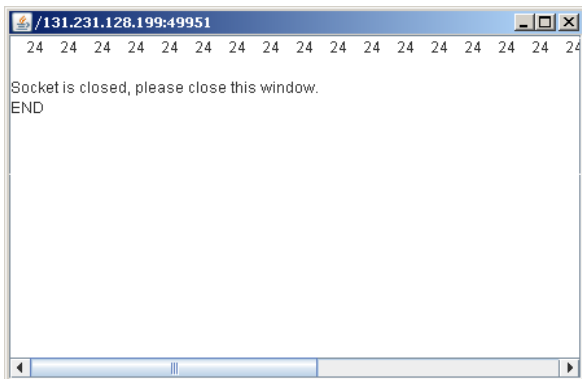


Figure 5. Sensor Gateway: new client connected

Using the demonstration system above, we found there are several disadvantages with the system. As a centralized

architecture, it is beneficial for indexing information. The user could easily find the sensor data they need from a central database. A sensor network works by following an on-demand model. A central database which requires the continuous updating of sensor information can significantly shorten the battery life of the sensor network nodes, which, in certain applications, very quickly run out of battery power. So a novel distributed approach linking a SOA (Service Oriented Architecture) with a federated sensor network has been created [9]. SOA (Service Oriented Architecture) is an evolution of the Component Based Architecture, in it, the functionality of the whole is divided up into smaller functions, each encapsulated within a component [10]. The new method is to consider all the sensor networks as a sensor service publisher and link them together to build a SOA system.

4 Distributed Federated Sensor Network

Distributed technology has shown great benefits in developing modern networks. Consider for example, a Distributed Data Server (DDS). This contains many data storage components distributed across multiple physical locations. The indexing service would only involve some of the storage components. This method could reduce the network traffic and thus save the computation resource. Another advantage of this system is that it is easy to upgrade and to maintain, because all of the distributed storage components are identical. Thus any one can be added to or replaced without affecting the others.

4.1 Distributed Federated Sensor Network description

A distributed federated sensor network is a unified system to collect, share, process and query sensor data from authorized sharing sensor networks. It aims to provide architecture, which general sensor networks can easily join and share the sensor data without requiring any modification to be made to the existing sensor network. Such system architecture is shown in *Figure 6*.

4.1.1 Sensor Networks

In an FSN, all different types of Sensor networks including wireless sensor network and static wired sensor network are acceptable. A new component called a Sensor Server Publisher (SSP) will be connected to an existing sensor networks. It is a special end device for reporting its own sensor network's characteristics, detailing available sensor data and uploading sensor data to the upper layer. The SSP is also a type of service provider. When it joins a sensor network it obtains a connection to the Internet or a specified network, the SSP can then search the Domain Sensor Name Server (DSNS) and register to it. Finally it records the sensor features. The sensor data transmission is active when it has received a request or exception sensor data has been detected. All the sensor data is directed to the Sensor Gateway, as the SSP do not have the ability to send data to multiple destinations.

4.1.2 Sensor Gateway

In a Federated Sensor Network, there is no restrictions on the kind of sensor network which can be included the sensing resources may be static when installed in buildings or on the roadside, or they may be mobile, if carried by humans or vehicles. Sensor networks may be based on many different platforms with different interfaces for access. Low power wireless sensor nodes may communicate via the IEEE 802.15.4 standard, while static sensor networks may have constant power supply to obtain higher bandwidth, reliability and life cycles so the interfaces can vary significantly. The Sensor Gateway provides a universal interface to all of the different types of sensor networks and implements specific methods to communicate with them. A Sensor Gateway is a PC based data transfer server, which is controlled by the DSNS. The applications are the direct consumers of the data. A database system can be included if required, and record incoming sensor data to meet the needs of future queries. There could be multiple Sensor Gateways in a Federated Sensor Network depending on the location of the sensor networks. For example a worldwide scale Federated Sensor Network would need at least one Sensor Gateway but could be extended to a maximum of 65,535 sensor networks. For an international FSN, at least one Sensor Gateway per nation is required to reduce the time delay caused by long distance data transmission.

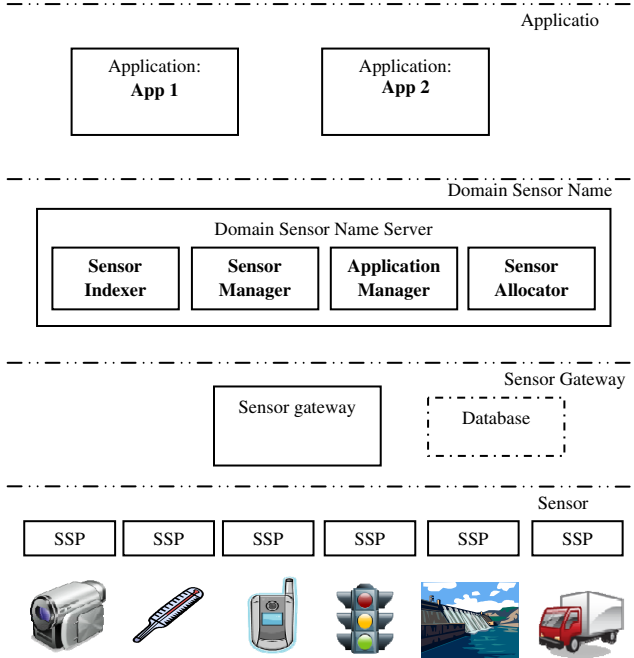


Figure 6. Distributed FSN architecture

4.1.3 Domain Sensor Name Server

The Domain Sensor Name Server is a sensor data central Indexing system. Its role is similar to that of the DNS on the Internet. The Domain Sensor Name Server translates the human language sensor descriptions such as the sensor types, location and logical names with the physical sensor identifiers and provides an index to

applications. There are four components of the DSNS: the Sensor Manager, the Application Manager, the Sensor Indexer and the Sensor Allocator.

- 1) The Sensor Manager is for sensor networks registration. It provides a mechanism for registering new sensor networks such as by defining the types, descriptions and name. In addition, it implements a management function for modifying the characteristics of previously registered sensor networks. The Sensor Indexer can use all the information collected in order to respond to a searching request from an application.
- 2) The Application Manager is designed to record the applications' information, such as the IP address, the application's details and the types of sensor data, which it is interested in. The reason to store this information is to notify applications when the sensor networks in which they have expressed an interest have captured exception data.
- 3) The Sensor Indexer provides a searching service for the sensor type or sensor characteristic to upper layer applications. The source of the index service comes from the Sensor Manager. It will search the sensor information when it has received a request from an application. If there is one or more sensor networks that can provide the specified type of sensor data, a positive response will be returned and the Sensor Allocator will be notified to arrange the data transmission.

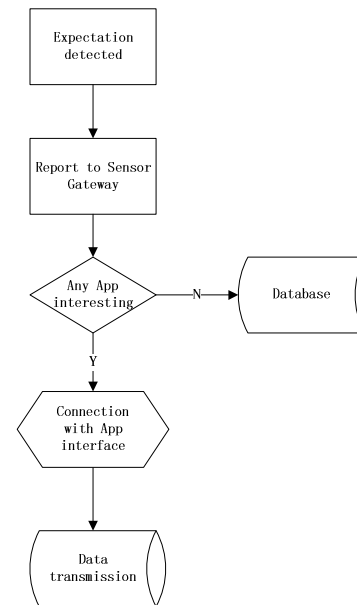


Figure 7. On demand queries

- 4) The Sensor Allocator is the most important and heavily loaded part of the DSNS. It serves as a connecting link between the applications and the Sensor Gateway. There are two types of events which may trigger the Sensor Allocator:
 - On demand queries (Figure 7): These occur once a sensor network has detected one or more exceptions and the data has been transmitted to

the Sensor Gateway. After that, The Sensor Gateway will report the sensor's property to the Application Manager to check whether there is any application interested. If there is, the Application Manager returns the application's connection information to the Sensor Allocator, the Sensor Allocator send a connection request with a listening port number and waits for the connecting response from the application. If there is no application interested, the Sensor Gateway stores the sensor data in the database for future use.

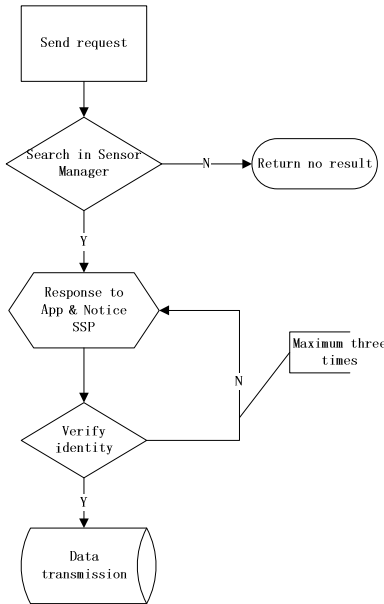


Figure 8. General queries

- General queries (Figure 8): The second type of query is when application sends a searching request to the Sensor Manager of the DSNS. If the sensor network can provide the data which the application is asking for, the Sensor Locator will return the specified sensor network's details including the IP address and the port number to the application, and it will also notify the SSP to activate the listening port for receiving connection requests from the application. There is a simple verifying mechanism for connection application to the sensor network. When the Sensor Locator returns the sensor network's details to the application and notifies the SSP to prepare for connection request, a randomly generated number will be sent to both of them. The application then sends a connection request containing this number. If the number matches, the connection will be accepted by the SSP otherwise it rejects the connection.

4.1.4 Applications Layer

Applications are the consumer of all the sensor data. They vary depending on different requirements. For example:

- An interactive application requires users to specify their data needs manually. For instance, there is an interactive GPS based navigator system installed in an ambulance. Once the address of a patient has been entered, the system should calculate the best route to that address. This process would require all the sensor data on or near the route, as any incident can cause traffic congestion that would delay the ambulance and endanger the patient's life. If incidents are detected the system should recalculate the route to avoid the incident location.
- An automated data collection system records the sensor data continuously and saves them for further analysis or indexing. For example, a supermarket management system obtains the volume of customer from the parking detector sensor network and determines shopper behaviours from the stock level using the sensor located under the items' shelf, and correlates them with the sales records.
- Google Maps is a globe mapping system that can provide navigating, local interest searching and many other convenient services. It also provides a useful platform for presenting sensor data, and can display the data from a non-private and non-sensitive sensor network to users directly without requiring the installation of any extra applications. Examples of data that might be displayed include the data from traffic sensor and fire detecting sensor. Google has announced the Google Maps API for any Maplet (small Google Maps build-in application) for their Google Maps service.

5 Comparison and Discussion

A Federated sensor network can assemble multiple types of sensor networks and supply sensor data to one or more applications for people to realize what is happening, and what is going to happen. Compares to the existing system, the distributed federated sensor network has three significant advantages which are identified as follows:

- 1) As it is constructed in a similar fashion to Service Oriented Architecture (SOA), the distributed federated sensor network can easily deal with on-demand data query without the large time delay that centralized federated sensor network exhibit. Because all the sensor networks have been implemented as small service providers, it omits the process of storing sensor data in a central database and directly builds connection to individual sensor network.
- 2) As a normal end device of the Internet, the Sensor Server Publisher does not have the ability to simultaneously forward data to different destinations. That means that the Sensor Server Publisher cannot serve multiple applications simultaneously. The Sensor Gateway works as a switch in the LAN,

which enables the forwarding of sensor data to different applications.

- 3) A distributed FSN has greater compatibility. In a centralized FSN, the database continuously extracts data from the sensor networks. However, a major problem with wireless sensor network is the limitation of their power supply, in other words the centralized FSN design is more suitable for a sensor network with a stable power supply. The distributed FSN is a decentralized system, which optimizes on-demand query for wireless sensor network. The sensor data is transmitted only when requires. This approach is beneficial for extending the battery life of wireless sensor networks.

6 Conclusions

A federated sensor network is able to provide more information than a normal sensor networks. At any time a user can monitor the environment variables, which are detected by different sensor networks in different zones. In this paper, we presented a demonstration of a centralized Federated Sensor Network, and then proposed an improved system architecture which combined the distribute technology with a Service Oriented Architecture. The development of distributed Federated Sensor Network is currently taking place and details of the proposed system will soon be published. It contains four major components: a Sensor Service Provider to publish the sensing service and transmit the sensor data to the upper layer (Sensor Gateway or applications); a Sensor gateway for making up the deficiency of SSP in feeding multiple targets; a Domain Sensor Name Server which works as an organizer in the system. The sensor service indexer takes requests from the applications for a search of a particular sensor type, and then it returns the sensor network's detail in order to establish a connection; finally, the applications are the sensor data consumers in the system. Compare with the previous system, the distributed federated sensor network has greater adaptability for sensor networks. It is more compatible with the characteristic of way the data circulates within a sensor network. The distributed architecture reduces the network load and enables different sensor network to work collaboratively. The Sensor Gateway enables multiple applications to simultaneously extract sensor data from one or more sensor networks. Finally, it is a multi to multi network. The entire system extends the usability of sensor networks and presents an effective design for a federated sensor network.

References

- [1] Archana Bharathidasan, Vijay Anand Sai Ponduru. Sensor networks: An Overview. University of California, Davis, CA 95616. Link: <http://www.wcsif.cs.ucdavis.edu/~bharathi/sensor/survey.pdf>
- [2] Römer, Kay; Friedemann Mattern (December 2004). "The Design Space of Wireless Sensor Networks". IEEE Wireless Communications 11 (6): 54–61. doi:10.1109/MWC.2004.1368897.
- [3] Feng-Yuan Ren, Hai-Ning Huang, Chuang Lin. Wireless Sensor Networks. 2003 Journal of Software, 1000-9825/2003/14(07)1282.
- [4] Bonnet P, Gehrke J, Seshadri P, Towards sensor database systems, Cornell University. Publisher: Springer Berlin / Heidelberg , ISBN 978-3-540-41454-4.
- [5] Bonnet P, Gehrke J, Querying the Physical World, 2000 IEEE Personal Communications, Volume: 7 Issue:5, ISSN: 1070-9916.
- [6] Suman Nath (main contact), Aman Kansal, Feng Zhao, SenseWeb, By Microsoft Research, Link: <http://research.microsoft.com/en-us/projects/senseweb/>
- [7] Andre Santanche, Suman Nath, Jie Liu, Bodhi Priyantha, Feng Zhao, SenseWeb: Browsing the Physical World in Real Time, Microsoft Research, Link: <http://www.cs.umd.edu/class/fall2009/cmsc828r/PAPERS/IPSNO6-SenseWeb%5B1%5D.pdf>
- [8] Ran Xu, Shuang-Hua Yang, Federated Wireless Sensor Network, Loughborough University, the 15th CACSUK 2009, ISBN 978-0-9555293-4-4.
- [9] Elena Meshkova, Janne Riihijärvi, Frank Oldewurtel, Christine Jardak and Petri Mähönen, Service-Oriented Design Methodology for Wireless Sensor Networks: A View through Case Studies, RWTH Aachen University, 2008 IEEE International Conference.
- [10] Service Oriented Architecture white paper, adobe Japanese enterprise link: http://www.adobe.com/jp/enterprise/pdfs/Services_Oriented_Architecture_from_Adobe.pdf