A CommonSense Approach to Real-world Global Sensing

Srdjan Krco, Mattias Johansson, Vlasios Tsiatsis
Ericsson
{srdjan.krco, mattias.a.johansson, vlasios.tsiatsis}@ericsson.com

Abstract: *In this paper we present our view of sensor and actuator networks, how we position them relative to the network of the future and what support such networks would both bring to and require from the existing and future core network. We put a special emphasis on the support infrastructure, and describe our envisioned architecture for a future ubiquitous sensor and actuator framework*

1. Introduction

Sensing and interacting with the physical world have gained a lot of attention during the last decade, which has resulted in a range of useful application proposals that have exploited the context of a person, an object or an area, to provide better services to users or enterprises. However, since these applications often served immediate and specialized needs (e.g. maps showing nearby restaurants or busy intersections) they were designed as *isolated* enclaves, i.e. as closed, standalone systems built with one specific purpose in mind. Some parameters of these sensor and actuator networks (further referred to as sensor networks) such as context information (*e.g.* general monitored area) and provided information type/format were predefined and preprogrammed into the applications. The full exploitation of the opportunities for *interaction* with other sensor networks to improve the coverage or context accuracy or opportunities for *data reuse* of and *data aggregation* across such application-specific and rigid systems is still remaining. If these opportunities are not addressed in time, they will turn into a problem which will definitely exacerbate as the number and total coverage of such installations increases.

In the realm of the network of the future, people, sensors, objects and spaces will be intertwined in both virtual and physical realms while collaborating and sharing information in an unobtrusive manner. WSNs will create new enriched services as well as enhance the existing communication services (person-person, person-machine, mobile-machine, person-content, and machine-machine). As a result, the role of sensor networks in the network of the future is to provide the missing link between the virtual and the physical world. Since most of today's sensor network infrastructures serve academic, enterprise or social groups either free of charge or using simple charging models, their design does not have any enablers for an open business environment. Along with this major challenge, several other challenges have to be overcome before such a ubiquitous communication, computing, sensing and actuation environment can be created. In this paper we build on our previous work on interconnecting wireless sensor networks with the support from mobile networks [1] and present our view of the architecture of a ubiquitous sensing and actuation framework that addresses some of the challenges mentioned above (*e.g.* business enablers, horizontal design, scalability, interoperability etc).

2. Related work

In this paper we make the first step towards a real world sensing framework that encourages business based on sensor/actuator services. We believe that the related work focused more on providing specialized systems for academic or social usage and less on enabling business based on sensor/actuators.

Both the Urban Sensing [2] and the MetroSense projects take a mobile phone centric approach and consider scenarios where sensing nodes are not owned by a small number of central authorities, but by citizens who carry sensors and contribute data voluntarily via their mobile devices. The Urban Sensing project aims to develop an architecture that will facilitate development of citizen-initiated sensing applications in personal, urban and social domains. The main three issues addressed are verification, privacy and dissemination. The MetroSense studies the large-scale deployment of mobile people-centric sensors and their interaction with embedded static sensor webs; the concept of opportunistic tasking, sensing, and fusion; and security, trust, and privacy.

The SensorPlanet [4] is a global research framework on mobile device-centric large scale wireless sensor networks. It explores suitable architectures to integrate sensor enhanced mobile phones and devices into mobile networks and make them available to mobile applications.

The SenseWeb [5] project aims to provide a common platform and set of tools that will allow easy publication of data from geographically distributed wireless sensor networks and making useful queries to the live data sources via a web service interface.

The Hourglass [6] project aims to build a scalable, robust data collection system to support geographically diverse sensor network applications. It creates an overlay infrastructure that provides service registration, discovery, and routing of data streams from sensors to one or more client applications.

The SANY [7] and CoBIS [8] projects focus on the development of an architecture that integrates wireless sensor networks into service oriented software architectures.

3. Motivation and requirements

Traditionally, wireless sensor networks are considered as autonomous installations deployed by one entity (an individual or an organization) with a specific purpose in mind and for a known group of users. The users have prior knowledge about the existence of the sensor network, of the type of information a particular sensor network can provide (for example temperature, air quality, etc.) and in many cases of the general coverage area of a sensor network. Interaction between a deployed network and the parties outside the jurisdiction of the organization that deployed the network is generally not envisaged. Also, interactions of the deployed network with other sensor networks deployed in the same area by other organizations for the purpose of ensuring higher accuracy, better coverage, cost reduction or even more context to the sensed data are traditionally not considered either.

Thanks to the technological advances, sensing hardware is becoming more and more portable, affordable and intelligent which make the deployment of small or large WSNs simple and easy even for people without significant technical knowledge. These factors in combination with the usefulness of the sensor based applications in many domains will inevitably lead to wide spread deployments of various sensor networks and their applications.

At the same time, the number of mobile subscribers is rising steadily for a number of years. Today, there are around 3 billion mobile subscriptions and as many mobile devices served by virtually globally accessible mobile networks. These mobile devices are powerful communication and computing multipurpose devices that are increasingly being equipped with a number of different sensors: image, sound, light, temperature, acceleration, RFID readers etc. The ability to interact with sensors in their vicinity via built-in short-range communication interfaces like Bluetooth, in addition to the previously mentioned characteristics, make mobile devices an excellent platform for sensing the physical environment and interacting with it.

3.1. Global collaboration and sensing

Inevitably, as these individual installations capable of sensing and actuating the world around them evolve, they will begin to interact, communicate, and exchange information. Similarly to the mash-ups created on Internet today, that combine different web services to provide added value to their customers, mash-ups of the individual sensor network installations will be created to provide context to observed events, more accurate observations, better coverage, faster reaction etc. as well as to enhance and enrich other services with available context information. Such interactions will open up possibilities for a number of new applications, will lead to introduction of new roles and players on the market, but will also bring a number of challenges and requirements for the underlying networks.

We expect that this new application and communication space will develop as an open information market where sensor information will be shared, contributed to community and social services, but also sold to interested parties. Sensor information providers (analogous to individual web services today, like Google Maps) will be ubiquitous, ranging from individuals carrying sensors on their bodies, in their pockets and cars, to sensors embedded into everyday objects that opportunistically use mobile phones and similar devices as gateways, to organizations using sensor information to support their internal business processes, to commercial sensor network operators deploying sensor networks of different types where and when they see business potential, i.e. where and when there is a need for specific information from a large number of users. The underlying networks, in particular mobile networks as ubiquitous access enablers providing global connectivity, will facilitate interaction between the information sources, sensor mash-up providers and the users of the information they produce.

3.2. Scalability & heterogeneity

As the sensor networking technology adoption drives the increase in the number of sensor network installations, an envisioned sensor and actuator framework should cope with the proliferation of both sensor networks in terms of *numbers* and *diversity*.

3.3. Plug & play

To build such an all-sensing environment, the sensor data contribution process, i.e. the process for making sensor data accessible and available to others, has to be as simple as possible. The architecture has to support seamless and dynamic addition of new sensors into the existing networks as well as changes in the functionality and capabilities of the existing sensor networks. The sensor owners should be involved as little as possible in individual transactions between the remote entities and the sensors. Instead, these transactions have to comply with the rules and policies defined by the sensor owners.

3.4. End user service delivery

The end users will access applications using a variety of devices, ranging from standard desktop PCs to mobile phones to purposely built terminals. Since the capabilities of these devices vary considerably the application providers will have to take that into account to deliver services in an appropriate format. IMS [9] is seen as a universal service delivery platform that provides support for a number of services and devices including authentication, location and charging mechanisms. Therefore, we expect to see further development in the IMS area to provide the additional functionality required by sensor based services.

3.5. Multiple usages

In many of today's deployed sensor solutions it is only possible to use the deployed sensor networks for one particular purpose. If one wants to deploy a new service, change service provider etc., the sensor networks must also be exchanged. With this model many possible services become too expensive to deploy. In the future, end users should be able to deploy their own sensor nodes, and then utilize this same set of sensor nodes for a very large set of services and applications that evolve over the lifetime of the sensors.

3.6. Security, privacy and trust

In an environment like this, where a huge number of small entities are opportunistically providing bits of information that are used as the basis for creation of high level services, it is important to use only reliable and trustworthy sources. At the same time it is equally important for the information sources to keep their privacy when providing data. It should not be possible for the application providers, or the end users, to pinpoint individual information sources used in creation of a service. Mobile networks already have in place authentication mechanisms, which in combination with their location tracking capabilities, represent an excellent starting point for building the required procedures.

3.7. Business models and incentives

We expect that today's rather static business models will change and adapt to the extremely dynamic environment expected in the future. There are several reasons for that. First, the end users will have only a small set of applications they subscribe to and use every day. They will access and use all other applications opportunistically, when and where required. Therefore, it is required to have a business solution in place that can facilitate numerous, small ad-hoc financial transactions between the users and application providers that take place in the background without significant user involvement. Secondly, the question of providing incentives to sensor network owners to make their networks available and accessible has to be resolved. Obviously, upload of sensor data towards application providers will incur some cost for using network resources. In some scenarios, like community and social networks, the sensor owners might be willing to bear that cost in return for the access to the community/social network application. However, if the sensor data is used in creation of a commercial service, remuneration will have to be provided to sensor network owners for the information they provide. Obviously, commercial sensor application providers could deploy their own sensor networks and basically create a closed business system. Although feasible, with the mass deployment of sensors we see a need to provide mechanisms and incentives to everyone to contribute the information they have to ensure as large coverage and diversity of information possible. Application providers will in such a scenario use different sensor networks at different times to create new services *e.g.* dynamic sensor mash-ups). The value of sensor network contribution will be variable depending on the relative importance of the information for a given application determined by the sensor accuracy, location, number of other similar sensors etc. The business model has to take all this factors into account and provide a fair remuneration to each sensor network involved in providing the service.

3.8. Enhancing existing services

The sensor based world should not be studied in isolation of other communication services. Mobile phones will not only gather and provide sensor information to remote applications and users, but will also use this input to enhance and enrich all other communication services that the mobile phone supports. For example, during a voice conversation, mobile devices can generate flower scents when the caller is in a garden.

3.9. New traffic models

Last, but not the least, new applications and services in combination with significantly increased number of network users will create new traffic patterns and will put new requirements on the underlying networks. This is particularly significant for wireless networks where radio resources are limited and where networks are not currently designed for such scenarios.

4. CommonSense architecture description

The proposed architecture is based on the requirements described above. We particularly focus on a horizontal approach and describe it first from a general viewpoint, then discuss the involved roles and finally we present it from a layered technological angle.

4.1. Horizontal approach

As has previously been stated, multiple applications will opportunistically interact with and query sensor

networks that at a given moment can produce required information. Obviously, different applications may require data from the same sensor networks. To avoid multiple end-to-end network data exchange, we see a need for an intermediary broker and processing layer. The entities in this layer will take care of interaction with individual sensor networks on one side, caching data for certain period of time to minimize network data flows and providing a unified sensor network interaction interface to applications on the other side. This kind of layer will play the role of the *narrow convergence waist* between the underlying heterogeneous sensor networks and the applications with diverse requirements on top of the narrow waist.

In the course of service creation, the service providers (sensor mash-ups) will process and aggregate data in an application specific manner. At the same time a number of common functions, like average over time and location, will be used as well. Since the data provided by the sensor networks will be channeled through the broker and processing layer it is expected that the entities comprising this layer will also perform a number of these common processing and data aggregating functions for all applications, thus reducing both the amount of data sent over the networks and the complexity of the applications.

4.2. Roles

To achieve the horizontal approach, there is a strong need to decouple sensor networks from the end user services. We shall strive to view sensors and actuators as resources that provide certain simple services that can be utilized to create more complex services over the lifetime of the sensor node. However, this does not mean that they are uncontrolled – free for anyone to use for whatever purpose. Security, privacy and trust are design goals that must always be prioritized. The sensors are still owned by a single administrative and business entity, either individual or organization, and this entity defines sensor network access and utilization policies, i.e. who gets what information and under which circumstances. This establishes the notion of a **WSN provider**, the entity providing the sensor network and its services.

On the other hand we have the business entities that provide higher level services to the end-users by combining and processing different sensor networks services and other required input like Google Maps. These entities collect the information, process it, and then display it for the user, order some actuation tasks or simply store the information for the future use. The possibilities are endless. We refer to these entities as **Service providers**.

What is missing to achieve a secure architecture enabling a real-time market for sensor based services is a business entity providing the aforementioned broker and processing layer functionality. This entity helps the service providers to find a sensor network, enforces access policies set by individual WSN providers, processes the data received from multiple sensor networks before delivering it to the requesting service provider, and provides authentication, accounting and billing functionality. This entity is the nave in our horizontal architecture and is referred to as the **CommonSense provider**. It is expected that there will be a multiplicity of CommonSense providers with different geographical spreads and specialties and with established business relationships between them to allow for a worldwide broker and processing layer.

The role of the CommonSense provider is to provide a unified interface to services provided by heterogeneous *sensors* and *actuators*. The CommonSense providers will collaborate with other entities such as location providers, telematics information providers, presence providers etc. These entities, referred to as the **3rd party service providers**, will process collected information in a specific manner or will be adding own information to the mix, thus providing additional value to the services provided by the CommonSense providers. In reality, these entities are often extensions of the current and already existing application enablers and networks such as OMA Location Server [10].

For a comprehensive view on the different roles and their relationships, see *Figure 1*. A number of WSN providers attach to different CommonSense providers, who in turn attach to service and 3rd party service providers. These attachments, shown in the figure as lines, actually represent both information transport and business interfaces. An interface between different administrative CommonSense providers enables the establishment of a distributed global framework for WSN access.

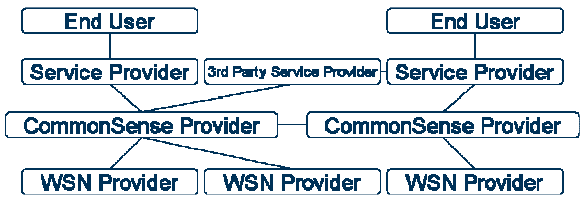

Figure 1: Roles and their relationships

4.3. Service oriented architecture

We propose a tiered service oriented architecture (SOA). The service providers interact with the CommonSense provider, who in turn is the entity directly interacting with the WSNs. The service providers treat the CommonSense provider as an entity providing services, and thus have no direct knowledge or influence over how the CommonSense provider finds the appropriate data to respond to their requests.

This constitutes the first level of the service architecture. The CommonSense provider then in turn treats the individual WSNs as entities offering services. This means that the sensor networks have to be able to describe themselves, where they are and what they can offer.

Note that traditional SOAs focus mainly on peer-to-peer workflow driven processes. In our architecture we instead envision that individual, moving WSNs offer very thin atomic and dynamic services while the CommonSense provider offers more complex services by combining these primitive WSN services to create for example mash-ups (see RA below).

There are multiple reasons for this tiered architecture. The first is that we wish to create a scalable system where the focus is not on every single individual sensor, but rather collections of them offering a service. Secondly, focusing on services only we become independent of specific sensor network implementations as long as these networks are able to describe how the service they provide can be used. Thirdly, we recognize the problem for an autonomous device to manage multiple dynamic security associations and the associated authorization decisions and we therefore propose to outsource the authorization task to the CommonSense provider - something which is enabled by the tiered SOA.

4.4. Architectural planes

The proposed architecture is mapped on three technology planes, see *Figure 2*: Communication services, Application enablers and Application plane. Applications are built using common service blocks residing in the Application enablers plane and all are connected by a number of network solutions residing in the Communication services plane.

Different domains are identified on each plane. The WSN, CommonSense and 3rd party service domains comprise the service plane, while the Peripheral, Access and Core domains comprise the Communication Services plane. In the Applications plane we differentiate between existing applications that do not depend on physical world context (e.g. call setup) and applications that cannot exist without one (e.g. burglar alarm).

We expect that multiple entities will occupy each domain. They will be working as a group according to a set of dynamically agreed business rules and will be providing services to entities in other domains of the same plane or to entities in other planes. The service interfaces between the domains on a plane will enable the creation of complex service blocks (CommonSense entities will combine a number of atomic WSN services to create more complex service blocks, sensor mash-ups, to applications). Business interfaces between domains on the same plane or across planes, will ensure the creation of an open service market facilitating fair remuneration to all entities involved in providing support to an application.

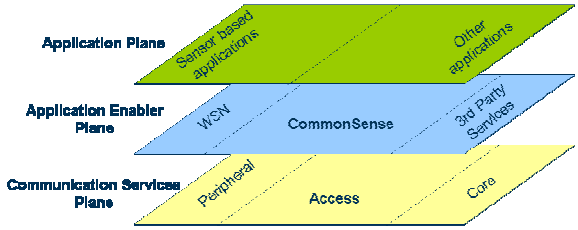

Figure 2: The proposed layering in our architecture

4.4.1. Application plane

The application providers providing end user applications reside on the application plane. They will use common service interface to issue high level queries (for example "What is the air quality in the main street") and receive responses from the Application enablers plane. The received responses will then be processed in an application specific manner and presented to the end users. Examples of applications are health and fitness applications, telematics and navigation applications, insurances, alarms of different kinds etc.

4.4.2. Application enablers plane

The Application enablers' plane is divided into three domains as described previously. The WSN domain comprises all atomic sensor services, i.e. services provided by individual sensors or sensor networks and used as small building blocks of more complex services offered by the entities residing in the CommonSense domain.

The CommonSense domain is where the core functionality of the proposed architecture resides. This domain does not host any specific applications, but provides a set of enablers for all types of applications. These enablers include information exchange, sensor network discovery, data processing, aggregation of atomic sensor network services (sensor mash-ups), Authentication, Authorization and Accounting (AAA) services. In short, the domain creates the possibility of having a dynamic binding between applications and WSNs. It is mainly based on semantic technologies which provide access independency. A single attachment point for sensor networks also facilitates security and privacy support.

We have defined a set of needed core functionalities in the CommonSense domain. These functions will be implemented in a distributed fashion across multiple business entities. The most important function is the Service Control Function (SCF) (*Figure 3*), which controls the interaction with all external parties. High level service requests from applications are analyzed by

the SCF with the support from the Request Analyzer (RA) and sensors, sensor networks or existing sensor mash-ups. The Request Analyzer (RA) is a decision engine that can decompose a request from an application to multiple individual information requests, and then recompose an aggregated answer. Of particular importance to the RA are functionalities such as planning, tasking, inference and data processing. The SR is a database containing registration descriptions of all attached WSNs. The description of a WSN contains three parts: available services, access policies and useful query attributes such as geographical coverage or position. The output from the RA is used to search the SR and find WSNs with matching capabilities. Once suitable WSNs are identified, the SCF issues either standardized low level service requests or special legacy WSN requests using a mediating function (see SGW below)

The SCF also interacts with the AAA functionality on the Application enablers plane in order to authenticate service providers and WSNs. The AAA also performs the accounting for compensation purposes and is the main enabler of sensor information as a market place.

The WSN provider functionality on the Application enablers plane is represented by Service Gateways (SGW). The SGW represents atomic sensor network services and is responsible for mapping the SCF requests onto the sensor network technology specific commands, which is a core requirement for interoperability. The SGW also provides functionality to host possible local intelligence (e.g. conditions and actions) pushed by CommonSense domain. This functionality can contribute to the efficient usage of communication network resources.

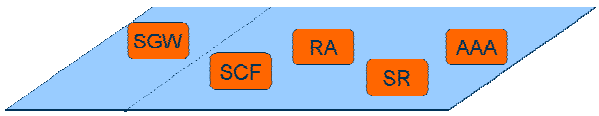

Figure 3: A deeper look at the CommonSense plane

The CommonSense domain entities will use 3rd party services as an additional tool in creation of application responses. The applications can also use the 3rd party services directly if it is required by the application logic. Some of the already existing services provided by the network are considered as the 3rd party services in the network of the future. Examples of the 3rd party service providers are presence servers, location providers, object identity resolution providers, etc.

4.4.3. Communication services plane

The communication services plane provides the underlying secure and reliable communications services to the Application enablers and the Application plane and enables interaction of all their entities across the different domains. The Communications service plane is divided into three domains: Peripheral refers to the local connectivity functionality (e.g. Bluetooth, Zigbee), Access refers to the wireless and wired last hop connectivity functionality (e.g. WCDMA, ADSL) and Core refers to the actual backbone.

It is an important architecture design goal that this plane should not be impacted by the business model, and therefore the required functionality should be independent of the Application enablers plane.

5. Conclusions

This paper presented our vision of a sensor and actuator framework in the context of the network of the future. Our architecture enables interoperability and scalability between a diverse set of applications and a vast number of underlying heterogeneous sensor networks while providing the right functionality for enabling business processes between the application providers and the sensor network owners or operators. As we envision that a large percentage of data exchange between the involved entities in our framework will be facilitated by mobile networks, the mobile networks themselves seem an obvious choice for hosting and providing the intermediary functionality of our architecture.

References

[1] S. Krco, D. Cleary, D. Parker, “Enabling ubiquitous sensor networking over mobile networks through peer-to-peer overlay networking”, *Computer Communications*, *Vol. 28, Issue 13*, *August 2005*, Elsevier.

[2] CENS Urban Sensing: http://research.cens.ucla.edu/projects/2006/Systems/Urban_Sensing/

[3] S.B. Eisenman, *et al*, “MetroSense Project: People-Centric Sensing at Scale”, World-Sensor Web, 2006, Boulder, Colorado.

[4] Sensor Planet: http://www.sensorplanet.org/index.html

[5] SenseWeb: http://research.microsoft.com/research/nec/SenseWeb/

[6] J. Shneidman, *et al*, “Hourglass: An Infrastructure for Connecting Sensor Networks and Applications”, http://www.eecs.harvard.edu/~syrah/hourglass/index.shtml

[7] EU FP6 Project SANY: http://sany-ip.eu

[8] EU FP6 Project CoBIs: http://www.cobis-online.de

[9] G. Camarillo, M.-A. García-Martín, "The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds", John Wiley & Sons, 2004.

[10] OMA Mobile Location Protocol (MLP) V3.1, http://www.openmobilealliance.org