Docusign Envelope ID: 26B008F2-A776-4258-9D33-26E4CA926FDF

DECLARATION OF GORDON MACPHERSON

I, Gordon MacPherson, am over twenty-one (21) years of age. I have never been convicted of a felony, and I am fully competent to make this declaration. I declare the following to be true to the best of my knowledge, information, and belief:

1. I am the Director, Board Governance & Policy Development at The Institute of Electrical and Electronics Engineers, Incorporated ("IEEE").
2. IEEE is a neutral third party in this dispute.
3. I am not being compensated for this declaration and IEEE is only being reimbursed for the cost of the article I am certifying.
4. Among my responsibilities as Director of Board Governance & Policy Development, I act as a custodian of certain records for IEEE.
5. I make this declaration based on my personal knowledge and information contained in the business records of IEEE.
6. As part of its ordinary course of business, IEEE publishes and makes available technical articles and standards. These publications are made available for public download through the IEEE digital library, IEEE Xplore.
7. It is the regular practice of IEEE to publish articles and other writings including article abstracts and make them available to the public through IEEE Xplore. IEEE maintains copies of publications in the ordinary course of its regularly conducted activities.
8. The article below has been attached as Exhibit A to this declaration:

Exhibit A	V. Tsetsos, G. Alyfantis, T. Hasiotis, O. Sekkas and S. Hadjiefthymiades, "Commercial Wireless Sensor Networks: Technical and Business Issues," *Second Annual Conference on Wireless On-demand Network Systems and Services*, St. Moritz, Switzerland, 2005, pp. 166-173, doi: 10.1109/WONS.2005.8.

9. I obtained a copy of Exhibit A through IEEE Xplore, where it is maintained in the ordinary course of IEEE's business. Exhibit A is a true and correct copy of the Exhibit as it existed on or about January 14, 2025.
10. The article and abstract from IEEE Xplore show the date of publication. IEEE Xplore populates this information using the metadata associated with the publication.

11. V. Tsetsos, G. Alyfantis, T. Hasiotis, O. Sekkas and S. Hadjiefthymiades, was published in "Commercial Wireless Sensor Networks: Technical and Business Issues," Second Annual Conference on Wireless On-demand Network Systems and Services, held in St. Moritz, Switzerland, on January 19-21, 2005. Copies of the conference proceedings were made available no later than the last day of conference. This article is currently available for public download from the IEEE digital library, IEEE Xplore.

12. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. § 1001.

I declare under penalty of perjury that the foregoing statements are true and correct.

Date: 1/17/2025

By: Signed by: Gordon MacPherson 845214E4A5C0470...

Commercial wireless sensor networks: technical and business issues

Publisher: IEEE Cite This PDF

V. Tsetsos ; G. Alyfantis ; T. Hasiotis ; O. Sekkas ; S. Hadjiefthymiades All Authors

13 Cites in Papers
19 Cites in Patents
170 Full Text Views

Abstract

Document Sections

1. Introduction
2. Sensor-Based Services
3. Network architecture of the SBS model
4. Business modeling issues
5. The software architecture of the SBS provisioning framework

Show Full Outline

Authors
Figures
References
Citations
Keywords
Metrics
More Like This
Footnotes

Abstract:
In this paper we study the opportunities of commercial exploitation of applications based on sensor networks. Such applications are quite famous nowadays in many different domains of everyday life (e.g., health monitoring, traffic monitoring). We introduce a new business model for sensor based services. Such business model involves entities like the mobile network operator and capitalizes on existing standards for application service providers (e.g., the OSA/Parlay standard). We also present the required technical framework that would facilitate the introduction and rapid adoption of the proposed business schemes.

Published in: Second Annual Conference on Wireless On-demand Network Systems and Services

Date of Conference: 19-21 January 2005

DOI: 10.1109/WONS.2005.8

Date Added to IEEE *Xplore*: 31 January 2005

Publisher: IEEE

Print ISBN:0-7695-2290-0

Conference Location: St. Moritz, Switzerland

SECTION 1.
Introduction

In the last few years, we have noticed a significant evolution of the mobile telecommunication networks and services. Nowadays, 2.5G mobile networks are the standard in most developed countries, whereas the penetration of 3G networks is steadily increasing (although slower than expected). This evolution was followed by an evolution of the provided services. New and innovative data services have shown up, which enhance the application environment of the end users. Probably the most promising of them are Location Based Services (LBS). LBS adapt the content provided to the users according to their physical location.

During these years, we have also witnessed an increasing interest of the research community in the wireless sensor networks (WSN) [3]. Such networks are the descendants of Micro Electro-Mechanical Systems (MEMS) and interconnect sensor nodes in order to provide a flexible topology for the dissemination of the sensed contextual information (e.g., temperature, motion, vibration). Since their invention, the WSNs have been mainly used in specific application domains such as habitat monitoring [4] (animal tracking, microclimate studies) and military surveillance applications.

By observing the above evolutions, one can predict that the ubiquitous environment of the future will comprise publicly and privately deployed sensor networks, which will enable the deployment of “smart services”, accessible through advanced infrastructures (e.g., the capability-rich 3G mobile networks or open services gateways). We strongly believe that this is a one-way scenario, judging from:

- the current user demand for context-aware services [10],
- the mobile market economics (market players seek for innovation through new services and killer applications) and,

Ex.1009 / Page 3 of 20
AMAZON.COM, INC.

- the vision for pervasive environments, which are highly interactive and responsive [5] (e.g., smart spaces, intelligent classrooms).

In the following sections we discuss how such a Sensor-Based Services (SBS) model, which combines (mobile) telecommunication technologies and WSNs, can be realized. In Section 2, we study the proposed Sensor Based Services (SBS) provisioning system. In Section 3, we study technical issues related to the proposed network architecture. In Section 4, we will study the economic aspects (revenue flows) of this new service model. Our current technology research towards the realization of this model is described in Section 5. The major problems that still prevent its wide and successful adoption are described in Section 6. The paper concludes with related work and future research directions.

SECTION 2.
Sensor-Based Services

Two typical scenarios that illustrate our view on the integration of sensor infrastructures (both private and public) in public mobile networks are the following:

Scenario A: Agy, a 3G mobile user, wants to monitor the healthcare (physical and biological state) of her grandmother, Sophie. For that purpose she orders her Mobile Network Operator (MNO) to install a full health-sensing system in Sophie's environment (house and body). Such system monitors her heart-pulse rate, body temperature, periodically takes photographs from the rooms and detects falls. Thus, Agy can periodically check Sophie's state and ensure that she is OK. In case of an emergency she will be notified through the Multimedia Messaging Service (MMS) push functionality provided by the MNO.
Scenario B: The vehicles of a country carry sensors according to the regulatory safety mandates. These sensors are powered by the main battery and monitor some operational parameters including speed (e.g., digital tachographs) and engine status. Some of these parameters are used only by the internal vehicle automation system (e.g., engine status) while others (e.g., speed) are also transmitted to adjacent nodes/cars through an RF module. Thus, all the cars in a specific region form an ad hoc wireless sensor network. Local authorities or the central government have installed gateway nodes in selected fixed positions (e.g., outside schools) that aggregate the sensed data and transmit them to a central system, along with the vehicle IDs, through the public mobile networks (alternatively, the police vehicles could carry such gateways). In this manner, dangerous drivers could be timely detected and penalized accordingly.
The above scenarios identify a major categorization of the possible WSN deployments: sensor networks can be either *private* or *public*. A private sensor network is deployed after a specific customer order to address her specific needs and thus it *can* and *should* be used only by this customer. In this case, the mobile network operator simply provides a secure bearer for the communication between the user endpoints. A public sensor network is deployed after a third-party's initiative and can be either of public unconstrained use or can be used by specific authorities for the public welfare. An example of a public WSN is the ad hoc sensor network of Scenario B, which monitors the traffic status so as to cater for public road safety. Other examples of both private and public deployments are sensor-enabled rescue teams, requiring ad hoc cooperation of their members, homeland security and medical applications.

Scenario A bears some resemblance to the LBS provisioning scenarios of the contemporary mobile networks. Firstly, they both deal with context-aware applications. In the case of LBS, the context is the user location, while for SBS, the context consists of the sensed environmental parameters (e.g., temperature). Secondly, the user registers for a health monitoring service similarly to the way she would register for a “traditional” data service, and receives the corresponding information either through a “pull” or a “push” model. In addition, the bearer of the service data in Scenario A is MMS, a widely used service today. However, significant differences do exist. For instance, the aforementioned WSN is a network deployed exclusively for the users directly involved in the scenario (i.e., the grandmother and its relatives) and, thus, it constitutes a private infrastructure. On the other hand, the positioning infrastructure of the mobile networks is at public disposal (obviously this assumption holds only in case of a network-based positioning method, since GPS-based methods rely on the user terminal [12]). Another difference is that the contextual information (sensor data) does not have the role of the content differentiator but it is the content itself, as opposed to location information that is usually used as a content selection criterion.

Ex.1009 / Page 4 of 20
AMAZON.COM, INC.

Although the WSN-related scenarios seem more futuristic and harder to realize than the LBS scenarios, this is not exactly the case. Firstly, the contextual information provided by a WSN is more accurate than the estimation of the user's location by a LBS system. This is mainly due to the imprecise positioning methods available today. Indeed, the lack of location accuracy is one of the main barriers that hinders the usability and penetration of the current location-aware services. Another promising characteristic of SBS is that, in general, they address more vital user needs than LBS. For example, environmental monitoring, healthcare monitoring, home security or remote industrial control, are regarded as more important and economically cost effective than a friend tracking service or a “find nearest restaurant” service. In other words, the added value for the user is much higher in the case of SBS.

The selection of a wireless sensor network instead of a (wired) static sensing infrastructure is a key decision in the service provisioning process. The WSN is highly flexible as it can be attached to mobile objects (e.g., wearable temperature sensors in Scenario A, carmounted sensors in Scenario B) and can be easily adapted to the considered problem. This adaptation is achieved by means of topological change, ad hoc network interoperation, and failure recovery (self-healing). This flexibility can be further translated into higher-level flexibility in the form of service differentiation, quality of service, ease of management, etc.

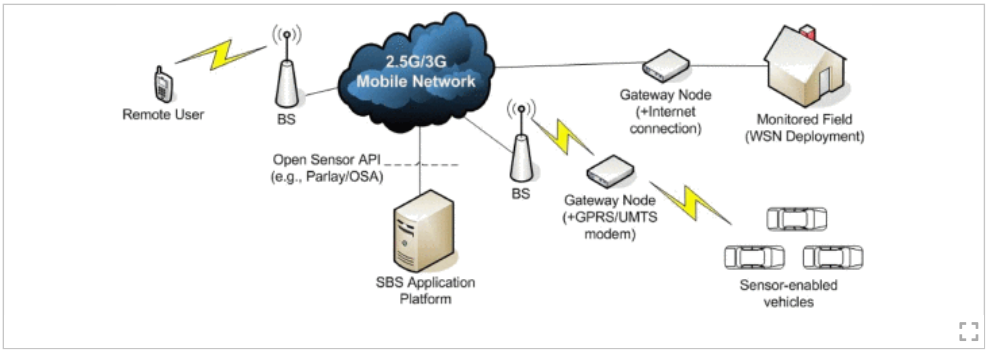


Figure 1. Enabling Sensor-Based Services in mobile networks

One possible question is the involvement of a mobile operator in the SBS provisioning. Firstly, we believe that the ubiquitous connectivity and the universal access provided by modern and forthcoming mobile networks, along with the high usability of the modern and next generation handsets, are unique features of flexibility that cannot be provided to the end users in other ways. Moreover, as the costs of use for these networks are constantly decreasing and the available bandwidth increases, they can be considered comparable to many of the already deployed wired networks.

SECTION 3.
Network architecture of the SBS model

The foundational technical similarities between the LBS and the SBS systems indicate that only minimal changes should be performed in an already deployed service provisioning network that aspires to provide truly context-aware services. Figure 1 depicts the general architecture of a SBS solution based on a 2.5G or 3G network.

The main modifications to the traditional network architecture will be:

A. The deployment of sensor networks in the monitored fields

A typical modern sensor network consists of sensor nodes and a gateway node. The gateway node has more processing, energy and communication capabilities than the other nodes and is the connecting link between the sensor network and the WAN (i.e., mobile network or Internet). Hence, this node should be capable of communicating with the mobile network infrastructure, either directly (GSM/GPRS modem) or indirectly (Internet modem and Gateway GPRS Support Node - GGSN).

B. An application platform for the lifecycle management of the services and the handling of the remote sensor networks

Ex.1009 / Page 5 of 20
AMAZON.COM, INC.

This platform is analogous to the LBS provisioning platforms [11], [14] and is responsible for the creation, deployment, and management of the SBS and the WSN. Furthermore, this platform, as a central component of the overall architecture, can handle all the relevant charging and payment issues. Such platform should be open and support the largest possible number of underlying sensor network technologies.

C. An open Sensor API for the communication between the WSN and the platform

The accumulated experience from the wireless networking applications dictates the standardization and adherence to open public APIs for the interaction between the applications and the network elements. Since the WSN can be regarded as a network element, the support of de facto standards for the WSN handling (i.e., sensor data retrieval) by the platform seems both crucial and feasible. Such an API could be the Parlay/OSA (Open Services Access) [1]. The only extension that would be required is the addition of a Sensor SCS (Service Capability Server) to the Parlay/OSA specification. Surely, the ongoing WSN research activity and the diversity in the WSN implementations introduce problems on such SCS standardization, but we can expect that the specific domain will be more clear and stable in a few years.

The aforementioned enhancements to the network are not so extensive and have limited impact, because they do not make any unrealistic assumptions on the capabilities of the existing core network and do not imply any alterations to the existing mobile terminal equipment. Thus, the value added services based on such a solution, could experience a fast market penetration with minimal infrastructure investment. However, some other technical issues emerge, which could potentially prevent their introduction. Among them are standardization, security and privacy, which will be discussed in more detail in Section 6.

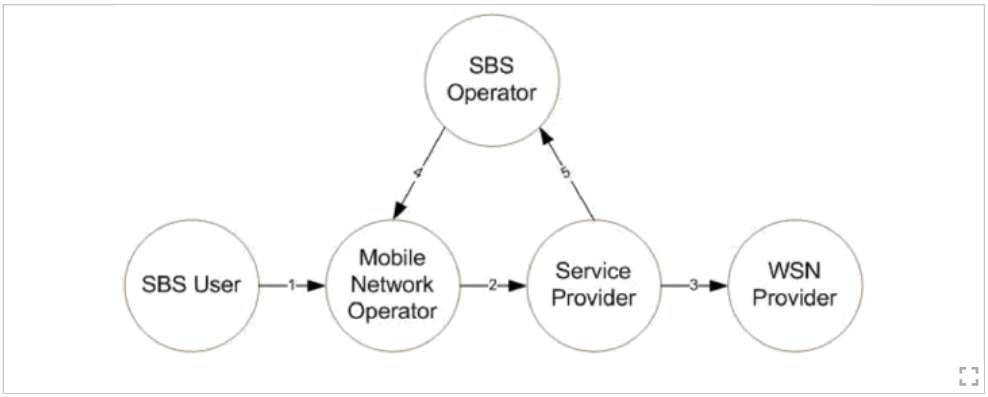


Figure 2. The revenue flows of the SBS model

SECTION 4.
Business modeling issues

4.1 Two new business roles

The network architecture in Figure 1 implies some changes in the value chain of this new service model. We propose that the greater part of the LBS value chain [15], [16] remains unchanged, but two new business roles should be introduced: the WSN Provider (WSNP) and the SBS Operator (SBSO).

A WSNP possesses the technical knowledge and capabilities for the physical deployment of the WSN. A WSNP may be a manufacturer of WSN hardware (and software) or may just be a technical company, which has the required know-how for the deployment and operation of WSNs. Hence, the WSNP will usually be unaware of the final applications. Among the responsibilities of the WSNP, apart from providing the necessary sensor and gateway equipment, is the provision of a "WSN driver" that conforms to the guidelines of the open Sensor API (see Figure 1). Such providers can deploy WSNs for either public or private use.

The second introduced role (SBSO) owns the SBS Application Platform and is responsible for the deployment of the Sensor-Based Services. For this purpose, it indirectly uses the "WSN driver" provided by the WSNP (through the Sensor API). The Service Providers, in turn, design and implement the context-aware services on this platform. In general, the role of the SBSO is similar to that of the LBS Operator that hosts the LBS provisioning platform (SBSO can be regarded as an Application Service Provider, ASP). SBSO provides a

Ex.1009 / Page 6 of 20
AMAZON.COM, INC.

service creation environment and all the software facilities necessary for the management of the service and WSN lifecycle. It may also sign contracts with the Mobile Network Operator (MNO) for the use of other network features, such as location servers. Finally, SBSO generates Charging Data Records (CDR) that can be used by the MNO for the final user charging and the accounting between the involved partners. There can be many different SBSOs over a single mobile network, just as there are many web hosting companies in the Internet. This ensures that the SBS market will be open and will provide the desired competitiveness.

4.2 A SBS business model

The introduction of these new players affects the revenue flows of the traditional service provisioning "ecosystems" as shown in Figure 2. With the term "traditional" we refer to the common telecom business models: a "strong" MNO, which outsources the creation of value added services to third-party Service Providers (SPs). In these business models there was no player similar to WSNP and there were no private deployments.

By tracing the revenue flows of the business model in Figure 2 we see that the SBS subscriber pays *directly* only the Mobile Network Operator (MNO) (flow 1). This provides convenience for the user, who does not have to deal with many different bills. At the same time, the role of the MNO is enhanced, as it can become a central payment handler. The MNO shares the user revenue with the Sp(s) (flow 2), which in turn pays the SBSO for the service hosting in the SBS platform (flow 5). The SP also pays the WSNP for the network deployment and other administrative activities (flow 3). Finally, the MNO charges directly the SBSO (flow 4) for the use of its communication facilities (e.g., sensor SCS, location servers) in the deployed services.

From the above model description we can observe that all the players incur an added value (AV) from the SBS provisioning. For the SPs, this AV comes from their closer relationship with the end-user, as they are *typically* (i.e., legally) responsible for the WSN deployment as well as the proper service operation (WSNPs have the actual responsibility for the WSN deployment and good performance). A SP may have contracts with a large number of WSNPs, specialized in different application domains (e.g., security, healthcare, etc.). In general, these WSNPs can be considered as "employees" of the SP, which in turn can be considered as an "employee"-partner of the MNO. The AV for the WSNPs is evident, as they only receive income for their services/products. The MNO also strengthens its position in the value chain as it gains from the additional provided services it provides to the subscribers and the possible payment services it provides to the other "players". Moreover, history teaches us that models that undermine the MNO's position in the value chain have no future. The mobile network is the central infrastructure in a SBS provisioning framework and MNOs will definitely rely on that in order to draw more profits and enhace their position in the market.

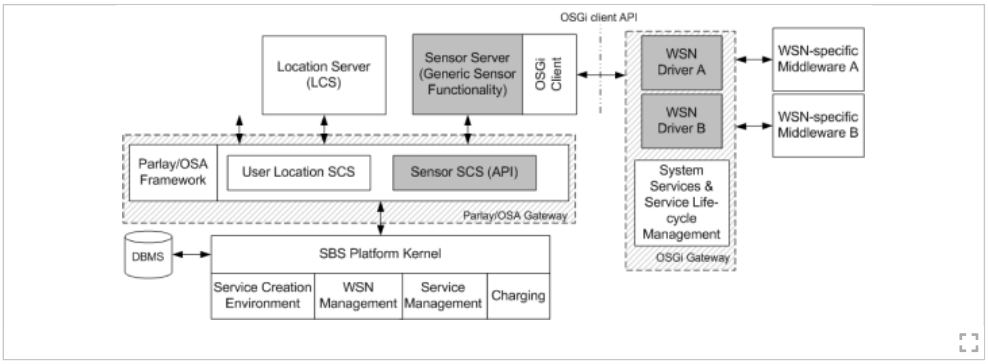


Figure 3. The distributed architecture of the overall SBS system

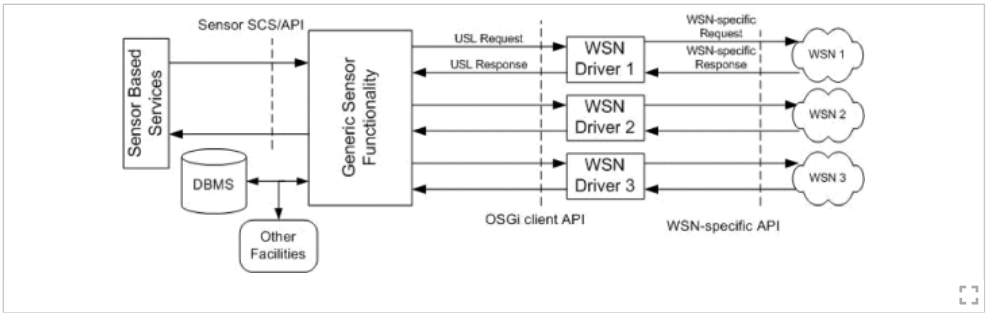


Figure 4. The proposed software architecture for SBS provisioning

Ex.1009 / Page 7 of 20
AMAZON.COM, INC.

SECTION 5.
The software architecture of the SBS provisioning framework

One major drawback of the current sensor networks is the lack of standards for both the lower network layers (i.e., physical, MAC, etc.) and the higher application layers. The current heterogeneity of the WSN technologies prevents their seamless use by ubiquitous services. We believe that, until the proper standards are set, a mediation layer (middleware) providing unified handling of these networks should bridge the gap.

In the case of telecommunication services, a good candidate for this mediation layer would be a combination of Parlay/OSA, and OSGi (Open Services Gateway Initiative) [2]. Parlay/OSA is a well-established industry standard, which, currently, is in its early adoption stages. The APIs specified by Parlay/OSA expose (almost) all the network functionality (user interaction, mobility management, user terminal capabilities, location, etc.) to application developers without compromising the overall network security. OSGi, on the other hand, was established in 1999 to define open specifications for the delivery and provisioning of multiple services over wide area networks to local networks and devices in homes, cars and other environments. The OSGi specifications try to standardize the secure and reliable service delivery and provisioning, for remote life cycle management of services, as well as for bridging between different networking standards. Until now, there have been several efforts in adopting OSGi as an open and standard platform for telematics services (see [13] for more references).

The general architecture of a SBS solution based on these specifications is depicted in Figure 3. Figure 3 shows how the various components of the architecture are distributed logically (their physical distribution can be inferred in conjunction with Figure 1). The main advantages of this solution are the independence of the application from the underlying WSN technology, the simple integration of sensor information in real-world applications (regardless of the application domain) and the adherence to standard specifications. Specifically, the Parlay/OSA interfaces, appropriately extended with a Sensor SCS/API, can provide developers with a common way for the interaction between the service logic and the actual sensor network. The mentioned Sensor SCS will also exploit other features of the Parlay/OSA Framework (e.g., charging, QoS, discovery). Furthermore, the OSGi Service Platform conceals the heterogeneity of the WSN technologies and enables their unified handling from the Parlay/OSA SCS through an OSGi Client API. Such API is not yet standardized but the MNOs have the potential to enforce its standardization process. In our opinion, such middleware brings the R&D community one step closer to the “Ambient Intelligence” [7], which envisages ubiquitous context-aware services. We are currently working on the implementation of such a middleware and, especially, on the components that appear in gray in Figure 3. Figure 4 shows in more detail the proposed middleware architecture, focusing only on these components, which are:

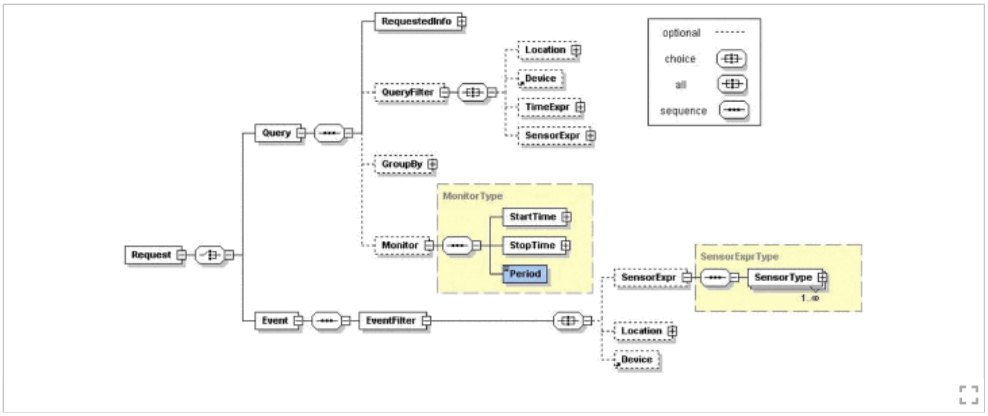


Figure 5. The XML Schema of USL Request

A. A high-level and developer-friendly Application Programming Interface (API)

that facilitates the development of context-aware services. This API is actually the Sensor SCS interface that was mentioned earlier and supports both event-driven (asynchronous) and query-based (synchronous)

Ex.1009 / Page 8 of 20
AMAZON.COM, INC.

interaction with the underlying WSNs. It also enables developers to store the sensor data in a DBMS and perform off-line and/or statistical post-processing on such data. The API takes into account the constraints of the WSNs, such as need for composite queries that reduce the transmitted data (and, thus, energy consumption), and promotes their use. The API, which is an interface to the Generic Sensor Functionality (GSF), is object-oriented and is based on a location model that eases the programming of context-aware services. For example, if we want to retrieve the (spatially) average temperature and the light intensity in office '19', we would create an object representing the region of the office and would invoke the method:

Off_I9.getSensorValue({AVG, NULL}, (TEMP, LIGHT })

where NULL means that we do not want the light intensity measurements to be aggregated (e.g., minimum, average, etc). The AVG aggregate in this example denotes a spatial average. In case of a temporal average we would also need older data stored in the DBMS.

B. The Generic Sensor Functionality (GSF) provided by sensor networks

which handles the developer's requests towards the WSN. This functionality maps the Parlay/OSA Sensor API to a general-purpose language, USL (Unified Sensor Language), and was resulted from an extended requirements analysis. This analysis aimed to address the widest possible variety of end-user requests, while taking into consideration the actual capabilities of the currently proposed WSN middleware [6] [7]. The USL specification, an XML Schema we are currently working on, describes two types of entities: *requests* for direct sensor retrieval or registration on sensor events, and *responses*, containing the actual sensor data or error messages returned from the network. A sample first version of the USL Request Schema is depicted in Figure 5, and a sample USL Request is presented in Listing 1. The listing demonstrates a request for a temperature sensor reading, from a sensor mounted on the device with ID 543.

GSF also integrates other facilities such as databases for sensor data post-processing and catalogs for discovery of available sensor networks.

C. A WSN driver

that partially consists of a USL parser. This driver parses the generated USL requests and translates them to WSN-specific code. For example, if we have a sensor network of TinyDB-enabled motes, the WSN driver would translate the USL requests to TinyDB [7] queries, would collect the TinyDB response, and would finally pass a corresponding USL response to the upper layers of the Sensor SCS. The deployment of the WSN driver in an OSGi Gateway located in the monitored field enables the aggregation of the sensor data and thus is more cost- and bandwidth-efficient. Additionally, OSGi fully supports the dynamic management of the WSN driver (e.g., remote installation of updates) and has been adopted by major industries (e.g., for vehicular telematics and home automation solutions).

```
<Request xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:noNamespaceSchemaLocation="
USLRequest.xsd" ID="123456">
  <Query>
    <RequestedInfo location="false" time-instance="false"
     device="true" sensor="true" time-duration="false">
      <SensorList>
        <SensorType function="NoFunction"
         type="temperature"/>
      </SensorList>
    </RequestedInfo>
    <QueryFilter>
      <Device ID="543"/>
    </QueryFilter>
  </Query>
</Request>
```

Listing 1. A sample USL Request

SECTION 6.
The difficulties behind SBS provisioning

The proposed commercialization plan for WSNs, although not very difficult to realize, cannot be thought of as tomorrow's reality. The main reasons for this are the lack of standards, regulation and the security holes of the WSNs, which enable privacy threats. The standardization of the WSN network stacks and the application-level interfaces has not even started yet, due to the ongoing research on these fields. Some efforts have been made with the IEEE 802.15.4 specification [9] (part of the ZigBee Alliance stack [19]), but they are covering only a narrow spectrum of issues (i.e., physical and data link layer protocols). In addition, the introduction of third parties (i.e., WSNPs), which have direct access to the user's personal information, can potentially constitute a substantial problem. The users will not be positive to cooperate with such parties and let them in their houses or vehicles, unless there is legal assurance that their sensitive data will not be disclosed for malicious purposes. Such assurance assumes the regulation of these issues on a governmental, or better international, level. Moreover, as the recent experience from the LBS has shown, the users will not adopt easily services with potential privacy threats. However, the situation for SBS is worse since the security threats in the physical, network and application layers are still poorly investigated [17], [18]. For example, eavesdropping is an easy task in current WSNs because most RF modules use simple modulations (e.g., FM), broadcast their messages and, in general, there is not cryptography support due to the physical limitations of the sensor nodes (energy, processing power and bandwidth). The insufficient support of the user's privacy increases the risk of the potential investments on these new markets and will postpone considerably the penetration of the SBS services.

SECTION 7.
Related Work

Although the vision for smart appliances and context-aware network services is not new, the industry and research institutes have not yet started to investigate the commercial coupling of sensor and telecommunication networks. This could be attributed both to the limited penetration of 3G services and to the sensor network open problems described in Section 6. An approach, which uses the OSGi Service Platform for the provision of context-aware automotive applications, is presented in [13]. In [20] a context-aware service provisioning platform for 3G networks is described. Some economic and business aspects of sensor networks are being studied in recently published commercial reports [21].

7.1 Case Studies

Some companies already provide commercial sensor nodes and software applications. Sensoria Corp. [22], for example, provides fault-tolerant sensor networking technologies, sensor nodes and open software platforms for sensor-based applications. Moreover, Crossbow Technology Inc. [23] has a great variety of WSN solutions (mainly hardware). The company is also cooperating with other end-to-end solution providers for the development of integrated systems. Some other relevant companies are Oracle Corp. [24], Intel Corp [25], and Sensicast Systems Inc. [26].

These companies/industries could potentially have the roles of WSNP, SBSO and/or SP. However, this is not the situation today for three reasons:

- The main products of all these companies address environmental monitoring, military applications, building/industrial automation and supply chain solutions. Thus, their target markets are industries and public sector agencies, and they lack support for customized end-user solutions.
- They have not exploited WSN deployment scenarios in cooperation with mobile network operators yet.
- There are no standard interfaces and platforms for the development of sensor-based services. The existence of such facilities would probably aid the introduction of SBS in wide area mobile networks.
- There is no regulation and legal framework for the provisioning of such services.

Ex.1009 / Page 10 of 20
AMAZON.COM, INC.

- The potential business models have not designed yet, since the technology barriers still exist.

SECTION 8.
Conclusions and Further Work

In this paper, we propose a model for the commercialization of the wireless sensor network through the provision of Sensor-Based Services for mobile subscribers. This architecture is based on existing open standards, (Parlay/OSA and OSGi), and introduces new middleware functionality, which enables the provision of the services and the handling of the sensor networks. In addition, we described a potential business model for such services. Finally, we discussed some problems, which hinder the realization of this new service model and could form future research directions. We are currently implementing the described middleware functionality and developing a prototype system for further experimentation. Such system could be further exploited for testing the business arrangements discussed in the paper.

Moreover, we plan to extend the proposed business model, in order to provide for service roaming; that is give the ability to customers to be free to "roam" from one MNO to another, without losing the sensor-based services they have subscribed for. Towards this direction we intend to explore whether well-established telecommunications business models and regulations (i.e., facilities similar to number portability) can be also applied for SBS.

Authors
Figures
References
Citations
Keywords
Metrics
Footnotes

IEEE Personal Account
CHANGE USERNAME/PASSWORD

Purchase Details
PAYMENT OPTIONS
VIEW PURCHASED DOCUMENTS

Profile Information
COMMUNICATIONS PREFERENCES
PROFESSION AND EDUCATION
TECHNICAL INTERESTS

Need Help?
US & CANADA: +1 800 678 4333
WORLDWIDE: +1 732 981 0060
CONTACT & SUPPORT

Follow

About IEEE *Xplore* | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | IEEE Ethics Reporting | Sitemap | IEEE Privacy Policy
A public charity, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2025 IEEE - All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies.

EXHIBIT A

Commercial Wireless Sensor Networks: Technical and Business Issues

Vassileios Tsetsos, George Alyfantis, Tilemahos Hasiotis, Odysseas Sekkas, and Stathes Hadjiefthymiades
Communication Networks Laboratory, University of Athens, Dept. of Informatics and Telecommunications, Panepistimiopolis, Ilissia, GR-15784, Athens, Greece
{b.tsetsos, g.alyfantis, thasiot, o.sekkas, shadj}@di.uoa.gr

Abstract

In this paper[1] we study the opportunities of commercial exploitation of applications based on sensor networks. Such applications are quite famous nowadays in many different domains of everyday life (e.g., health monitoring, traffic monitoring). We introduce a new business model for sensor based services. Such business model involves entities like the mobile network operator and capitalizes on existing standards for application service providers (e.g., the OSA/Parlay standard). We also present the required technical framework that would facilitate the introduction and rapid adoption of the proposed business schemes.

1. Introduction

In the last few years, we have noticed a significant evolution of the mobile telecommunication networks and services. Nowadays, 2.5G mobile networks are the standard in most developed countries, whereas the penetration of 3G networks is steadily increasing (although slower than expected). This evolution was followed by an evolution of the provided services. New and innovative data services have shown up, which enhance the application environment of the end users. Probably the most promising of them are Location Based Services (LBS). LBS adapt the content provided to the users according to their physical location.

During these years, we have also witnessed an increasing interest of the research community in the wireless sensor networks (WSN) [3]. Such networks are the descendants of Micro Electro-Mechanical Systems (MEMS) and interconnect sensor nodes in order to provide a flexible topology for the dissemination of the sensed contextual information (e.g., temperature, motion, vibration). Since their invention, the WSNs have been mainly used in specific application domains such as habitat monitoring [4] (animal tracking, microclimate studies) and military surveillance applications.

By observing the above evolutions, one can predict that the ubiquitous environment of the future will comprise publicly and privately deployed sensor networks, which will enable the deployment of "smart services", accessible through advanced infrastructures (e.g., the capability-rich 3G mobile networks or open services gateways). We strongly believe that this is a one-way scenario, judging from:

- the current user demand for context-aware services [10],
- the mobile market economics (market players seek for innovation through new services and killer applications) and,
- the vision for pervasive environments, which are highly interactive and responsive [5] (e.g., smart spaces, intelligent classrooms).

In the following sections we discuss how such a Sensor-Based Services (SBS) model, which combines (mobile) telecommunication technologies and WSNs, can be realized. In Section 2, we study the proposed Sensor Based Services (SBS) provisioning system. In Section 3, we study technical issues related to the proposed network architecture. In Section 4, we will study the economic aspects (revenue flows) of this new service model. Our current technology research towards the realization of this model is described in Section 5. The major problems that still prevent its wide and successful adoption are described in Section 6. The paper concludes with related work and future research directions.

[1] This work is supported by the PYTHAGORAS programme of the Greek Ministry of National Education and Religious Affairs (University of Athens Research Project No 70/3/7411)

Proceedings of the Second Annual Conference on Wireless On-demand Network Systems and Services (WONS'05)
0-7695-2290-0/05 $ 20.00 IEEE
Authorized licensed use limited to: IEEE - Staff. Downloaded on January 14,2025 at 19:39:54 UTC from IEEE Xplore. Restrictions apply.
IEEE COMPUTER SOCIETY

2. Sensor-Based Services

Two typical scenarios that illustrate our view on the integration of sensor infrastructures (both private and public) in public mobile networks are the following:

Scenario A - *Agy, a 3G mobile user, wants to monitor the healthcare (physical and biological state) of her grandmother, Sophie. For that purpose she orders her Mobile Network Operator (MNO) to install a full health-sensing system in Sophie's environment (house and body). Such system monitors her heart-pulse rate, body temperature, periodically takes photographs from the rooms and detects falls. Thus, Agy can periodically check Sophie's state and ensure that she is OK. In case of an emergency she will be notified through the Multimedia Messaging Service (MMS) push functionality provided by the MNO.*

Scenario B - *The vehicles of a country carry sensors according to the regulatory safety mandates. These sensors are powered by the main battery and monitor some operational parameters including speed (e.g., digital tachographs) and engine status. Some of these parameters are used only by the internal vehicle automation system (e.g., engine status) while others (e.g., speed) are also transmitted to adjacent nodes/cars through an RF module. Thus, all the cars in a specific region form an ad hoc wireless sensor network. Local authorities or the central government have installed gateway nodes in selected fixed positions (e.g., outside schools) that aggregate the sensed data and transmit them to a central system, along with the vehicle IDs, through the public mobile networks (alternatively, the police vehicles could carry such gateways). In this manner, dangerous drivers could be timely detected and penalized accordingly.*

The above scenarios identify a major categorization of the possible WSN deployments: sensor networks can be either *private* or *public*. A private sensor network is deployed after a specific customer order to address her specific needs and thus it *can* and *should* be used only by this customer. In this case, the mobile network operator simply provides a secure bearer for the communication between the user endpoints. A public sensor network is deployed after a third-party's initiative and can be either of public unconstrained use or can be used by specific authorities for the public welfare. An example of a public WSN is the ad hoc sensor network of Scenario B, which monitors the traffic status so as to cater for public road safety. Other examples of both private and public deployments are sensor-enabled rescue teams, requiring ad hoc cooperation of their members, homeland security and medical applications.

Scenario A bears some resemblance to the LBS provisioning scenarios of the contemporary mobile networks. Firstly, they both deal with context-aware applications. In the case of LBS, the context is the user location, while for SBS, the context consists of the sensed environmental parameters (e.g., temperature). Secondly, the user registers for a health monitoring service similarly to the way she would register for a "traditional" data service, and receives the corresponding information either through a "pull" or a "push" model. In addition, the bearer of the service data in Scenario A is MMS, a widely used service today. However, significant differences do exist. For instance, the aforementioned WSN is a network deployed exclusively for the users directly involved in the scenario (i.e., the grandmother and its relatives) and, thus, it constitutes a private infrastructure. On the other hand, the positioning infrastructure of the mobile networks is at public disposal (obviously this assumption holds only in case of a network-based positioning method, since GPS-based methods rely on the user terminal [12]). Another difference is that the contextual information (sensor data) does not have the role of the content differentiator but it is the content itself, as opposed to location information that is usually used as a content selection criterion.

Although the WSN-related scenarios seem more futuristic and harder to realize than the LBS scenarios, this is not exactly the case. Firstly, the contextual information provided by a WSN is more accurate than the estimation of the user's location by a LBS system. This is mainly due to the imprecise positioning methods available today. Indeed, the lack of location accuracy is one of the main barriers that hinders the usability and penetration of the current location-aware services. Another promising characteristic of SBS is that, in general, they address more vital user needs than LBS. For example, environmental monitoring, healthcare monitoring, home security or remote industrial control, are regarded as more important and economically cost effective than a friend tracking service or a "find nearest restaurant" service. In other words, the added value for the user is much higher in the case of SBS.

The selection of a wireless sensor network instead of a (wired) static sensing infrastructure is a key decision in the service provisioning process. The WSN is highly flexible as it can be attached to mobile objects (e.g., wearable temperature sensors in Scenario A, car-mounted sensors in Scenario B) and can be easily adapted to the considered problem. This adaptation is achieved by means of topological change, ad hoc network interoperation, and failure recovery (self-healing). This flexibility can be further translated into

Proceedings of the Second Annual Conference on Wireless On-demand Network Systems and Services (WONS'05)
0-7695-2290-0/05 $ 20.00 IEEE
Authorized licensed use limited to: IEEE - Staff. Downloaded on January 14,2025 at 19:39:54 UTC from IEEE Xplore. Restrictions apply.
IEEE COMPUTER SOCIETY

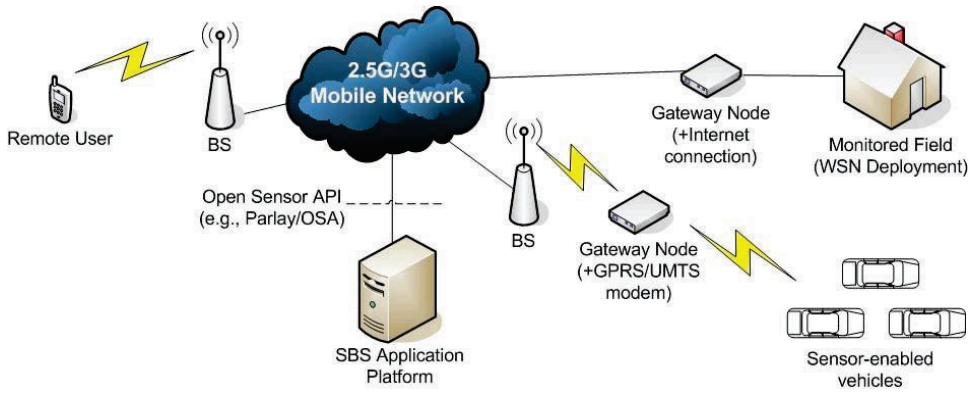


Figure 1. Enabling Sensor-Based Services in mobile networks

higher-level flexibility in the form of service differentiation, quality of service, ease of management, etc.

One possible question is the involvement of a mobile operator in the SBS provisioning. Firstly, we believe that the ubiquitous connectivity and the universal access provided by modern and forthcoming mobile networks, along with the high usability of the modern and next generation handsets, are unique features of flexibility that cannot be provided to the end users in other ways. Moreover, as the costs of use for these networks are constantly decreasing and the available bandwidth increases, they can be considered comparable to many of the already deployed wired networks.

3. Network architecture of the SBS model

The foundational technical similarities between the LBS and the SBS systems indicate that only minimal changes should be performed in an already deployed service provisioning network that aspires to provide truly context-aware services. Figure 1 depicts the general architecture of a SBS solution based on a 2.5G or 3G network.

The main modifications to the traditional network architecture will be:

A. The deployment of sensor networks in the monitored fields. A typical modern sensor network consists of sensor nodes and a gateway node. The gateway node has more processing, energy and communication capabilities than the other nodes and is the connecting link between the sensor network and the WAN (i.e., mobile network or Internet). Hence, this node should be capable of communicating with the mobile network infrastructure, either directly (GSM/GPRS modem) or indirectly (Internet modem and Gateway GPRS Support Node - GGSN).

B. An application platform for the lifecycle management of the services and the handling of the remote sensor networks. This platform is analogous to the LBS provisioning platforms [11], [14] and is responsible for the creation, deployment, and management of the SBS and the WSN. Furthermore, this platform, as a central component of the overall architecture, can handle all the relevant charging and payment issues. Such platform should be open and support the largest possible number of underlying sensor network technologies.

C. An open Sensor API for the communication between the WSN and the platform. The accumulated experience from the wireless networking applications dictates the standardization and adherence to open public APIs for the interaction between the applications and the network elements. Since the WSN can be regarded as a network element, the support of de facto standards for the WSN handling (i.e., sensor data retrieval) by the platform seems both crucial and feasible. Such an API could be the Parlay/OSA (Open Services Access) [1]. The only extension that would be required is the addition of a Sensor SCS (Service Capability Server) to the Parlay/OSA specification. Surely, the ongoing WSN research activity and the diversity in the WSN implementations introduce problems on such SCS standardization, but we can expect that the specific domain will be more clear and stable in a few years.

The aforementioned enhancements to the network are not so extensive and have limited impact, because they do not make any unrealistic assumptions on the capabilities of the existing core network and do not imply any alterations to the existing mobile terminal equipment. Thus, the value added services based on such a solution, could experience a fast market penetration with minimal infrastructure investment. However, some other technical issues emerge, which

Proceedings of the Second Annual Conference on Wireless On-demand Network Systems and Services (WONS'05)
0-7695-2290-0/05 $ 20.00 IEEE
Authorized licensed use limited to: IEEE - Staff. Downloaded on January 14,2025 at 19:39:54 UTC from IEEE Xplore. Restrictions apply.
IEEE COMPUTER SOCIETY

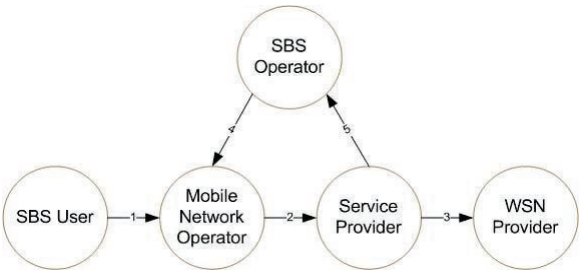


Figure 2. The revenue flows of the SBS model

could potentially prevent their introduction. Among them are standardization, security and privacy, which will be discussed in more detail in Section 6.

4. Business modeling issues

4.1 Two new business roles

The network architecture in Figure 1 implies some changes in the value chain of this new service model. We propose that the greater part of the LBS value chain [15], [16] remains unchanged, but two new business roles should be introduced: the WSN Provider (WSNP) and the SBS Operator (SBSO).

A WSNP possesses the technical knowledge and capabilities for the physical deployment of the WSN. A WSNP may be a manufacturer of WSN hardware (and software) or may just be a technical company, which has the required know-how for the deployment and operation of WSNs. Hence, the WSNP will usually be unaware of the final applications. Among the responsibilities of the WSNP, apart from providing the necessary sensor and gateway equipment, is the provision of a "WSN driver" that conforms to the guidelines of the open Sensor API (see Figure 1). Such providers can deploy WSNs for either public or private use.

The second introduced role (SBSO) owns the SBS Application Platform and is responsible for the deployment of the Sensor-Based Services. For this purpose, it indirectly uses the "WSN driver" provided by the WSNP (through the Sensor API). The Service Providers, in turn, design and implement the context-aware services on this platform. In general, the role of the SBSO is similar to that of the LBS Operator that hosts the LBS provisioning platform (SBSO can be regarded as an Application Service Provider, ASP). SBSO provides a service creation environment and all the software facilities necessary for the management of the service and WSN lifecycle. It may also sign contracts with the Mobile Network Operator (MNO) for the use of other network features, such as location servers. Finally, SBSO generates Charging Data Records (CDR) that can be used by the MNO for the final user charging and the accounting between the involved partners. There can be many different SBSOs over a single mobile network, just as there are many web hosting companies in the Internet. This ensures that the SBS market will be open and will provide the desired competitiveness.

4.2 A SBS business model

The introduction of these new players affects the revenue flows of the traditional service provisioning "ecosystems" as shown in Figure 2. With the term "traditional" we refer to the common telecom business models: a "strong" MNO, which outsources the creation of value added services to third-party Service Providers (SPs). In these business models there was no player similar to WSNP and there were no private deployments.

By tracing the revenue flows of the business model in Figure 2 we see that the SBS subscriber pays *directly* only the Mobile Network Operator (MNO) (flow 1). This provides convenience for the user, who does not have to deal with many different bills. At the same time, the role of the MNO is enhanced, as it can become a central payment handler. The MNO shares the user revenue with the SP(s) (flow 2), which in turn pays the SBSO for the service hosting in the SBS platform (flow 5). The SP also pays the WSNP for the network deployment and other administrative activities (flow 3). Finally, the MNO charges directly the SBSO (flow 4) for the use of its communication facilities (e.g., sensor SCS, location servers) in the deployed services.

From the above model description we can observe that all the players incur an added value (AV) from the SBS provisioning. For the SPs, this AV comes from their closer relationship with the end-user, as they are *typically* (i.e., legally) responsible for the WSN deployment as well as the proper service operation (WSNPs have the actual responsibility for the WSN deployment and good performance). A SP may have contracts with a large number of WSNPs, specialized in different application domains (e.g., security, healthcare, etc.). In general, these WSNPs can be considered as "employees" of the SP, which in turn can be considered as an "employee"-partner of the MNO. The AV for the WSNPs is evident, as they only receive income for their services/products. The MNO also strengthens its position in the value chain as it gains from the additional provided services it provides to the subscribers and the possible payment services it provides to the other "players". Moreover, history teaches us that models that undermine the MNO's

Proceedings of the Second Annual Conference on Wireless On-demand Network Systems and Services (WONS'05)
0-7695-2290-0/05 $ 20.00 IEEE
Authorized licensed use limited to: IEEE - Staff. Downloaded on January 14,2025 at 19:39:54 UTC from IEEE Xplore. Restrictions apply.
IEEE COMPUTER SOCIETY

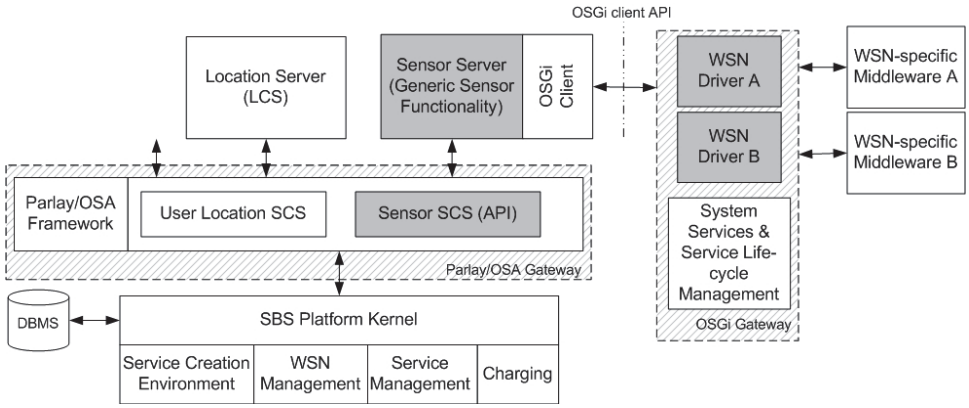


Figure 3. The distributed architecture of the overall SBS system

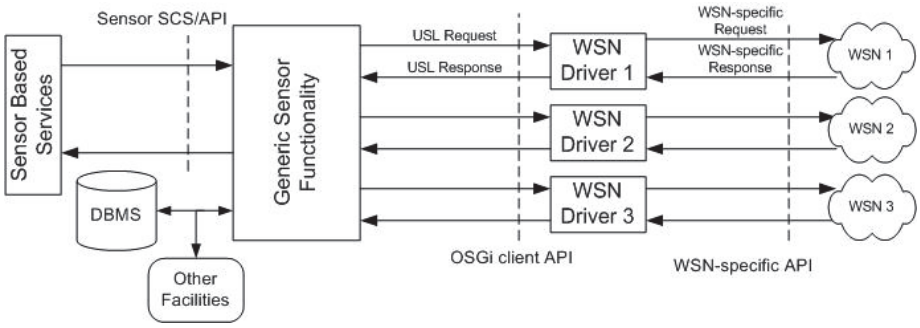


Figure 4. The proposed software architecture for SBS provisioning

position in the value chain have no future. The mobile network is the central infrastructure in a SBS provisioning framework and MNOs will definitely rely on that in order to draw more profits and enhace their position in the market.

5. The software architecture of the SBS provisioning framework

One major drawback of the current sensor networks is the lack of standards for both the lower network layers (i.e., physical, MAC, etc.) and the higher application layers. The current heterogeneity of the WSN technologies prevents their seamless use by ubiquitous services. We believe that, until the proper standards are set, a mediation layer (middleware) providing unified handling of these networks should bridge the gap.

In the case of telecommunication services, a good candidate for this mediation layer would be a combination of Parlay/OSA and OSGi (Open Services Gateway Initiative) [2]. Parlay/OSA is a well-established industry standard, which, currently, is in its early adoption stages. The APIs specified by Parlay/OSA expose (almost) all the network functionality (user interaction, mobility management, user terminal capabilities, location, etc.) to application developers without compromising the overall network security. OSGi, on the other hand, was established in 1999 to define open specifications for the delivery and provisioning of multiple services over wide area networks to local networks and devices in homes, cars and other environments. The OSGi specifications try to standardize the secure and reliable service delivery and provisioning, for remote life cycle management of services, as well as for bridging between different networking standards. Until now, there have been several efforts in adopting OSGi as an open and standard platform for telematics services (see [13] for more references).

The general architecture of a SBS solution based on these specifications is depicted in Figure 3. Figure 3 shows how the various components of the architecture are distributed logically (their physical distribution can be inferred in conjunction with Figure 1). The main advantages of this solution are the independence of the application from the underlying WSN technology, the simple integration of sensor information in real-world applications (regardless of the application domain) and

Proceedings of the Second Annual Conference on Wireless On-demand Network Systems and Services (WONS'05)
0-7695-2290-0/05 $ 20.00 IEEE
Authorized licensed use limited to: IEEE - Staff. Downloaded on January 14,2025 at 19:39:54 UTC from IEEE Xplore. Restrictions apply.
IEEE COMPUTER SOCIETY

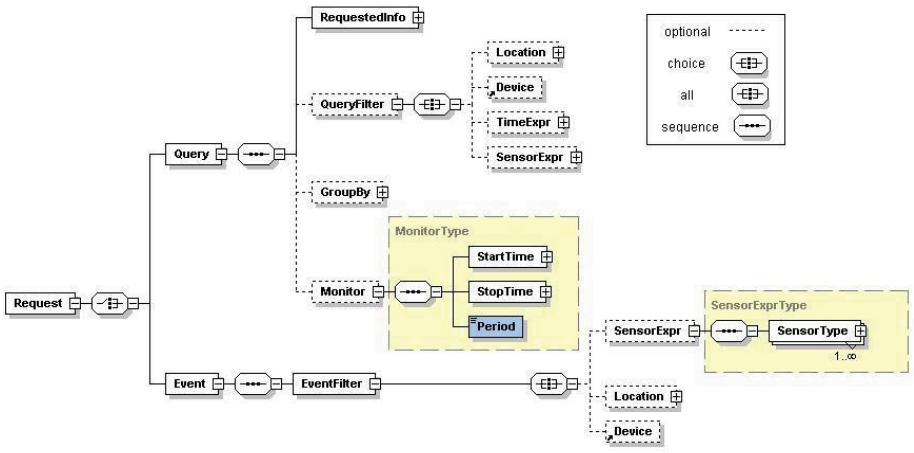


Figure 5. The XML Schema of USL Request

the adherence to standard specifications. Specifically, the Parlay/OSA interfaces, appropriately extended with a Sensor SCS/API, can provide developers with a common way for the interaction between the service logic and the actual sensor network. The mentioned Sensor SCS will also exploit other features of the Parlay/OSA Framework (e.g., charging, QoS, discovery). Furthermore, the OSGi Service Platform conceals the heterogeneity of the WSN technologies and enables their unified handling from the Parlay/OSA SCS through an OSGi Client API. Such API is not yet standardized but the MNOs have the potential to enforce its standardization process. In our opinion, such middleware brings the R&D community one step closer to the "Ambient Intelligence" [7], which envisages ubiquitous context-aware services. We are currently working on the implementation of such a middleware and, especially, on the components that appear in gray in Figure 3. Figure 4 shows in more detail the proposed middleware architecture, focusing only on these components, which are:

A. A high-level and developer-friendly Application Programming Interface (API) that facilitates the development of context-aware services. This API is actually the Sensor SCS interface that was mentioned earlier and supports both event-driven (asynchronous) and query-based (synchronous) interaction with the underlying WSNs. It also enables developers to store the sensor data in a DBMS and perform off-line and/or statistical post-processing on such data. The API takes into account the constraints of the WSNs, such as need for composite queries that reduce the transmitted data (and, thus, energy consumption), and promotes their use. The API, which is an interface to the Generic Sensor Functionality (GSF), is object-oriented and is based on a location model that eases the programming of context-aware services. For example, if we want to retrieve the (spatially) average temperature and the light intensity in office 'I9', we would create an object representing the region of the office and would invoke the method:

Off_I9.getSensorValue({AVG,NULL},{TEMP,LIGHT})

where NULL means that we do not want the light intensity measurements to be aggregated (e.g., minimum, average, etc). The AVG aggregate in this example denotes a spatial average. In case of a temporal average we would also need older data stored in the DBMS.

B. The Generic Sensor Functionality (GSF) provided by sensor networks, which handles the developer's requests towards the WSN. This functionality maps the Parlay/OSA Sensor API to a general-purpose language, USL (Unified Sensor Language), and was resulted from an extended requirements analysis. This analysis aimed to address the widest possible variety of end-user requests, while taking into consideration the actual capabilities of the currently proposed WSN middleware [6][7]. The USL specification, an XML Schema we are currently working on, describes two types of entities: *requests* for direct sensor retrieval or registration on sensor events, and *responses*, containing the actual sensor data or error messages returned from the network. A sample first version of the USL Request Schema is depicted in Figure 5, and a sample USL Request is presented in Listing 1. The listing demonstrates a request for a temperature sensor reading, from a sensor mounted on the device with ID 543.

GSF also integrates other facilities such as databases for sensor data post-processing and catalogs for discovery of available sensor networks.

Proceedings of the Second Annual Conference on Wireless On-demand Network Systems and Services (WONS'05)
0-7695-2290-0/05 $ 20.00 IEEE
Authorized licensed use limited to: IEEE - Staff. Downloaded on January 14,2025 at 19:39:54 UTC from IEEE Xplore. Restrictions apply.
IEEE COMPUTER SOCIETY

C. A WSN driver that partially consists of a USL parser. This driver parses the generated USL requests and translates them to WSN-specific code. For example, if we have a sensor network of TinyDB-enabled motes, the WSN driver would translate the USL requests to TinyDB [7] queries, would collect the TinyDB response, and would finally pass a corresponding USL response to the upper layers of the Sensor SCS. The deployment of the WSN driver in an OSGi Gateway located in the monitored field enables the aggregation of the sensor data and thus is more cost- and bandwidth-efficient. Additionally, OSGi fully supports the dynamic management of the WSN driver (e.g., remote installation of updates) and has been adopted by major industries (e.g., for vehicular telematics and home automation solutions).

```
<Request xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:noNamespaceSchemaLocation="
USLRequest.xsd" ID="123456">
   <Query>
      <RequestedInfo location=”false” time-instance=”false”
       device=”true” sensor=”true” time-duration=”false”>
         <SensorList>
            <SensorType function=”NoFunction”
             type=”temperature”/>
         </SensorList>
      </RequestedInfo>
      <QueryFilter>
         <Device ID=”543”/>
      </QueryFilter>
   </Query>
</Request>
```

Listing 1. A sample USL Request

6. The difficulties behind SBS provisioning

The proposed commercialization plan for WSNs, although not very difficult to realize, cannot be thought of as tomorrow’s reality. The main reasons for this are the lack of standards, regulation and the security holes of the WSNs, which enable privacy threats. The standardization of the WSN network stacks and the application-level interfaces has not even started yet, due to the ongoing research on these fields. Some efforts have been made with the IEEE 802.15.4 specification [9] (part of the ZigBee Alliance stack [19]), but they are covering only a narrow spectrum of issues (i.e., physical and data link layer protocols). In addition, the introduction of third parties (i.e., WSNPs), which have direct access to the user’s personal information, can potentially constitute a substantial problem. The users will not be positive to cooperate with such parties and let them in their houses or vehicles, unless there is legal assurance that their sensitive data will not be disclosed for malicious purposes. Such assurance assumes the regulation of these issues on a governmental, or better international, level. Moreover, as the recent experience from the LBS has shown, the users will not adopt easily services with potential privacy threats. However, the situation for SBS is worse since the security threats in the physical, network and application layers are still poorly investigated [17], [18]. For example, eavesdropping is an easy task in current WSNs because most RF modules use simple modulations (e.g., FM), broadcast their messages and, in general, there is not cryptography support due to the physical limitations of the sensor nodes (energy, processing power and bandwidth). The insufficient support of the user’s privacy increases the risk of the potential investments on these new markets and will postpone considerably the penetration of the SBS services.

7. Related Work

Although the vision for smart appliances and context-aware network services is not new, the industry and research institutes have not yet started to investigate the commercial coupling of sensor and telecommunication networks. This could be attributed both to the limited penetration of 3G services and to the sensor network open problems described in Section 6. An approach, which uses the OSGi Service Platform for the provision of context-aware automotive applications, is presented in [13]. In [20] a context-aware service provisioning platform for 3G networks is described. Some economic and business aspects of sensor networks are being studied in recently published commercial reports [21].

7.1 Case Studies

Some companies already provide commercial sensor nodes and software applications. Sensoria Corp. [22], for example, provides fault-tolerant sensor networking technologies, sensor nodes and open software platforms for sensor-based applications. Moreover, Crossbow Technology Inc. [23] has a great variety of WSN solutions (mainly hardware). The company is also cooperating with other end-to-end solution providers for the development of integrated systems. Some other relevant companies are Oracle Corp. [24], Intel Corp [25], and Sensicast Systems Inc. [26].

These companies/industries could potentially have the roles of WSNP, SBSO and/or SP. However, this is not the situation today for three reasons:

- The main products of all these companies address environmental monitoring, military applications, building/industrial automation and supply chain

Proceedings of the Second Annual Conference on Wireless On-demand Network Systems and Services (WONS’05)
0-7695-2290-0/05 $ 20.00 IEEE
Authorized licensed use limited to: IEEE - Staff. Downloaded on January 14,2025 at 19:39:54 UTC from IEEE Xplore. Restrictions apply.
IEEE COMPUTER SOCIETY

solutions. Thus, their target markets are industries and public sector agencies, and they lack support for customized end-user solutions.

- They have not exploited WSN deployment scenarios in cooperation with mobile network operators yet.
- There are no standard interfaces and platforms for the development of sensor-based services. The existence of such facilities would probably aid the introduction of SBS in wide area mobile networks.
- There is no regulation and legal framework for the provisioning of such services.
- The potential business models have not designed yet, since the technology barriers still exist.

8. Conclusions and Further Work

In this paper, we propose a model for the commercialization of the wireless sensor network through the provision of Sensor-Based Services for mobile subscribers. This architecture is based on existing open standards, (Parlay/OSA and OSGi), and introduces new middleware functionality, which enables the provision of the services and the handling of the sensor networks. In addition, we described a potential business model for such services. Finally, we discussed some problems, which hinder the realization of this new service model and could form future research directions. We are currently implementing the described middleware functionality and developing a prototype system for further experimentation. Such system could be further exploited for testing the business arrangements discussed in the paper.

Moreover, we plan to extend the proposed business model, in order to provide for service roaming; that is give the ability to customers to be free to "roam" from one MNO to another, without losing the sensor-based services they have subscribed for. Towards this direction we intend to explore whether well-established telecommunications business models and regulations (i.e., facilities similar to number portability) can be also applied for SBS.

9. References

[1] A.J. Moerdijk and L. Klostermann, "Opening the Networks with Parlay/OSA: Standards and Aspects Behind the APIs", *IEEE Network*, May 2003, pp. 58-64.

[2] OSGi Alliance Specification Overview, URL: http://www.osgi.org/resources/spec_overview.asp

[3] I. Akyildiz, et al., "Wireless sensor networks: a survey", *Computer Networks*, Elsevier, March 2002, pp.393-422.

[4] R. Szewczyk, et al., "Habitat monitoring with sensor networks", *Communications of the ACM*, 47(6), June 2004, pp. 34-40

[5] I. Essa, "Ubiquitous Sensing for Smart and Aware Environments", *IEEE Personal Communications, Special Issue on Networking the Physical World*, October 2000, pp. 47-49.

[6] C-C. Shen, C. Srisathapornphat, and C. Jaikaeo, "Sensor Information Networking Architecture and Applications," *IEEE Personal Communications*, August 2001, pp. 52-59.

[7] P. Levis, et al., "The Emergence of Networking Abstractions and Techniques in TinyOS", *First USENIX/ACM Symposium on Networked Systems Design and Implementation*, San Francisco, 2004.

[8] ISTAG, "Scenarios for Ambient Intelligence in 2010", Final Report, Feb 2001, EC 2001 URL: http://www.cordis.lu/ist/istag.htm

[9] J.A. Gutierrez, et al., *Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensors with IEEE 802.15.4*, IEEE Press, 2003

[10] L. Barkhuus, A. Dey, "Is Context-Aware Computing Taking Control Away from the User? Three Levels of Interactivity Examined", *Proceedings of UBICOMP 2003*, Seattle, May 2003, pp. 149-156.

[11] Telenity's Canvas™ Location Enabling Server, http://www.telenity.com/location_services.php

[12] G. Swedberg, "Ericsson's mobile location solution" *Ericsson Review No. 04*, 1999.

[13] D. Zhang, X. Wang, et al., "OSGi Based Service Infrastructure for Context Aware Automotive Telematics". *IEEE Vehicular Technology Conference*, Milan, Italy, May 2004.

[14] A. Ioannidis, et al., "PoLoS: Integrated Platform for Location-Based Services", *IST Mobile & Wireless Communications Summit*, Portugal, June 2003.

[15] J. Paavilainen, *Mobile Business Strategies,* Addison Wesley, 2002.

[16] P. Timmers, "Business Models for Electronic Markets", *Journal on Electronic Markets*, Vol 8, 1998, pp. 3-8.

[17] A. Perrig, et al., "SPINS: Security Protocols for Sensor Networks", *MOBICOM 2001*, Rome, Italy, June 2001.

[18] Sasha Slijepcevic, Vlasios Tsiatsis, Scott Zimbeck, "On Communication Security in Wireless Ad-Hoc Sensor Networks", *WETICE'02*, Pittsburgh, USA 2002.

[19] ZigBee Alliance, http://www.zigbee.org

[20] P. Costa, et al. "Towards a Services Platform for Mobile Context-Aware Applications", *First International Workshop on Ubiquitous Computing (IWUC 2004)*, Portugal, April 2004.

[21] ON World Inc., Wireless Sensor Networks: Mass market Opportunities, February 2004

[22] Sensoria Corp., http://www.sensoria.com

[23] Crossbow Technology Inc., http://www.xbow.com

[24] Oracle Sensor-Based Services http://www.oracle.com/technologies/rfid/index.html

[25] Intel Corp., http://www.intel.com

[26] Sensicast Systems Corp., http://www.sensicast.com

Proceedings of the Second Annual Conference on Wireless On-demand Network Systems and Services (WONS'05)
0-7695-2290-0/05 $ 20.00 IEEE

Authorized licensed use limited to: IEEE - Staff. Downloaded on January 14,2025 at 19:39:54 UTC from IEEE Xplore. Restrictions apply.