UNIVERSITY OF CAMBRIDGE
Cambridge Service Alliance

Using Smart Objects to build the Internet of Things

Tomás Sánchez López, Damith C. Ranasinghe, Mark Harrison, Duncan McFarlane

This paper was published in IEEE Internet Computing

Why this paper might be of interest to Alliance Partners:

The term Internet of Things (IoT) is a concept that encompasses a variety of technologies and research areas that aim to extend the existing internet to real world objects . Some of the potential benefits from the IoT realisation are enormous, both for individuals and businesses. Some of the most promising applications include: improved management of global supply chain logistics, product counterfeit detection, manufacturing automation, smart homes and appliances, e-government (electronic official document and currency), improved integrated vehicle health management and e-health (patient monitoring). This paper examines the technologies that will be fundamental for realising the Internet of Things (IoT) concept and proposes an architecture that integrates them into a single platform.

September 2012

UNIVERSITY OF CAMBRIDGE
Cambridge Service Alliance

Using Smart Objects to build the Internet of Things

Tomás Sánchez López, Damith C. Ranasinghe, Mark Harrison, Duncan McFarlane

The Internet of Things (IoT) concept is being widely presented as the next revolution towards massively distributed information, where any real world object can automatically participate in the Internet and thus be globally discovered and queried. Despite the consensus on the great potential of the concept, and the significant progress in a number of enabling technologies, there is a general lack of an integrated vision on how to realize it. This article examines the technologies that will be fundamental for realizing the IoT and proposes an architecture that integrates them into a single platform. The architecture uses the Smart Object framework to encapsulate radio-frequency identification (RFID), sensor technologies, embedded object logic, object ad-hoc networking and Internet-based information infrastructure. We demonstrate the architecture by detailing an implementation using Wireless Sensor Networks and Web Services, and describe a prototype for the real-time monitoring of goods flowing through a supply chain.

Introduction

The term Internet of Things (IoT) is a concept that encompasses a variety of technologies and research areas that aim to extend the existing Internet to real world objects [15]. The potential benefits from the IoT realization are enormous, both for individuals and businesses. Some of the most promising applications include: improved management of global supply chain logistics, product counterfeit detection, manufacturing automation, smart homes and appliances, e-government (electronic official document and currency), improved integrated vehicle health management and e-health (patient monitoring).

Automatic identification technologies such as RFID are fundamental players in the realization of the IoT because they enable physical objects to be linked with their virtual identity on the Internet. The ability to monitor the condition of things by means of sensors makes possible to react to changes on the status of the objects. Radio communication technologies and embedded processing increase the autonomy of the object by providing them with networking capabilities and local intelligence. Finally, distributed information infrastructures using Internet protocols for communication serve as a connection hub for all the 'things', together with other resources such as databases, data mining tools and computer networks.

The great amount of different technologies involved in the IoT concept represents an immense challenge and requires an effective integration framework. Although separate efforts in areas such as RFID and sensors have produced important results [1] [4], there is no existing platform that integrates all their functionalities. In this article we propose the Smart Object (SO) framework as an integration architecture that features the most important functionalities described earlier: Smart Objects are objects not only capable of providing their unique identification and condition, but also able to perform object-to-object communications, ad-hoc networking and object-centric complex decision-making. The SO framework is completed with an information infrastructure that leverages the SO feature set, providing users with access to both ID/sensor and SO network information by means of well-defined interfaces. Our objective in this article is thus to show how the combination of all the characteristics and features derived from this architecture addresses many of the challenges and applications of the Internet of Things.

Technology Background and Related Work

Rapidly evolving new applications, such as food safety and vehicle health management, are based on knowing the condition of objects (e.g., temperature, stress, strain, shock). Passive RFID has traditionally provided automatic object identification and the location at which the objects have been identified, while new directions in active and semi-passive RFID provide enhanced object identification functionalities with various degrees of autonomy [8]. Although RFID is an important technology in the realisation of a seamless link between individual physical objects and their digital representations, it can not provide the condition information that the next generation of real world applications require. Sensor technologies have emerged to fill these requirements, and their integration with wireless communication has produced research areas such as Wireless Sensor Networks (WSN), where miniaturized, energy-efficient battery-powered wireless devices serve as a platform for transmitting the sensor data [9]. A recent trend is to incorporate sensors into RFID tags [10]

Table I summarizes the most relevant related work, either on architectures that integrate RFID and sensors or on standardization efforts that we consider key towards the realization of the IoT. As Table 1 highlights, although the technologies for gathering, processing and distributing information about objects either already exist or are well advanced, there is little or no integration among them, leading to a lack of a comprehensive platform for heterogeneous data processing and sharing. In the rest of the article, we aim to introduce an architecture that not only includes the most important foreseen features of the IoT, but that also provides all the details for creating efficient and complete implementations. Our proposed architecture also includes new features such as context-based ad-hoc network and clustering of objects, which can potentially improve the quality and meaning of the collected data.

Table 1 – Summary of RFID and Sensor Integration Related Work

	Description	Main shortcomings	Potential improvements
PROMISE [3]	EU project using Product Embedded Information Devices (PEID) for monitoring ID and condition of objects during their life cycle	Little alignment with standards, no networking of PEIDs	Adoption of ID standards. Consider sensor (object) networking
OGC SWE [4]	Extensive set of protocols and interfaces to share sensor information in a standard way over the Internet.	IDs not globally unique. Sensors are not considered to monitor objects or products	
EPC Network [1]	Emerging industrial RFID standards architecture based on unique item identification via the Electronic Product Code (EPC)	Does not yet handle sensor data	Extend current standards with sensor data
BRIDGE [5]	EU project for developing new technologies within the EPC Network	Work with sensors does not extend the EPC Network	
EPC SN [7]	Auto-ID lab project to extend the EPC Network with sensors	Too complex to allow a full architecture extension	Compromise in developing a simpler functional part of the extension
ISO 18000.6, 24753, IEEE 1451.7	Set of standards dealing with the integration of RFID with sensors	Under development. Cooperation among standardization bodies is complex and slow	Standards need to reach a mature state before they can be used
GSN [13]	Middleware to collect and share information from RFID and WSN over the Internet	RFID and WSN data is not integrated at object level	Provisions for collecting both RFID and sensor data from an object
Mitsugi et al. [14]	General architecture for managing RFID and WSN integrated information	No description on real-world implementations	Further detail is needed to realize their vision
SARIF [11]	Middleware for designing applications requiring RFID and WSN information	Integration is only by spatial comparison, no mention of Internet scalability	Consider more integration methods and an explicit connection with Internet protocols

The Smart Object Framework

The basic concept behind the smart objects approach is to provide a single platform for the creation, processing and sharing of events based on both RFID and sensor data, as well as a mechanism for accessing object conditions and their contextual networks via well defined, Internet-based interfaces. This section introduces the SO framework and thus constitutes the core of our contribution.

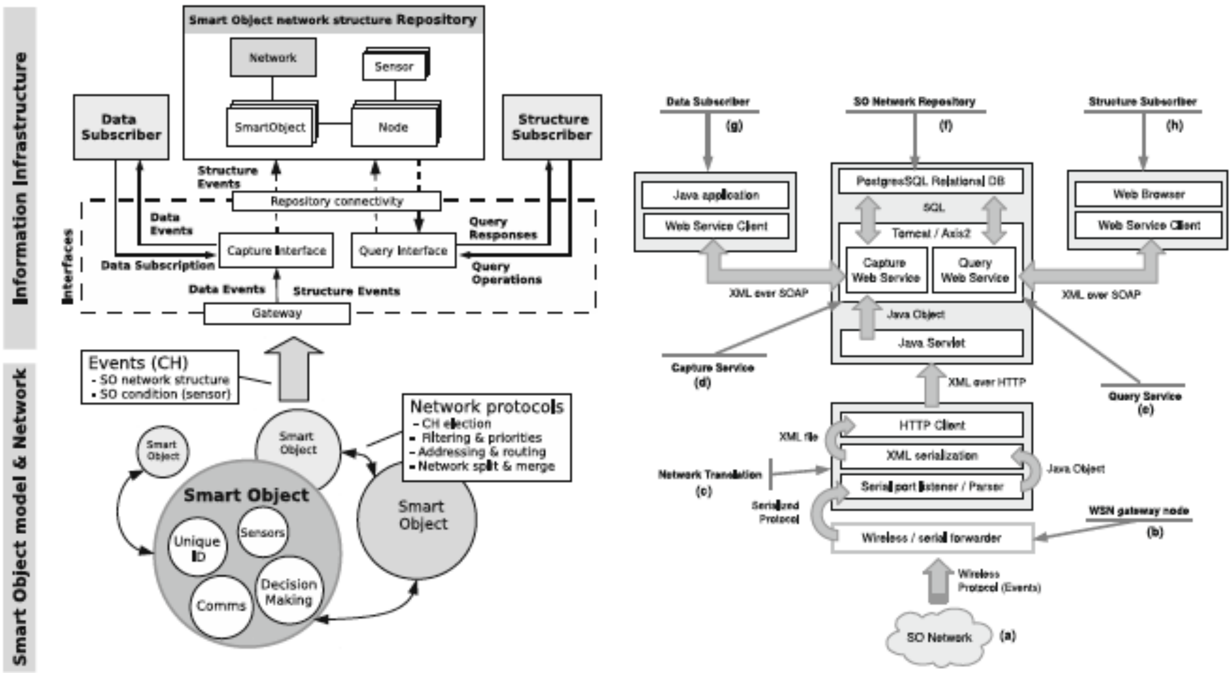
A. Smart Object definition

The integration of object identification and sensor data streams may be realized in multiple ways. For example it is possible to merge ambient sensory data provided by a sensorrich space to identities of objects entering that space by detecting when objects enter the area. However, this scenario might prove difficult to implement since detection systems must be placed on the boundaries of the space. Moreover, architectural logic must be put in place for merging both independent streams of data (sensor data and automatic identification data). Furthermore, sensor data could be deemed inaccurate since the transducers could be located at a considerable distance from the monitored objects.

With the new developments on integrated circuitry, microelectro-mechanical systems (MEMS), wireless communications and embedded technologies in general, the vision of an integration that occurs at the hardware level is more plausible and logical than ever. As the amount and type of information that can be embedded into assets increases, we witness an evolution towards object-centric systems, where manufactured items take control over the flow of information which was traditionally retrieved manually by human operators. As a result of the augmented capabilities and "intelligence" that the object-centric paradigm supports, this new generation of assets has been called smart products or, more generally, "smart objects". Our framework for building Smart Objects is based on five fundamental properties: Smart Objects are those objects that,

- possess a unique identity.
- are able to sense and store measurements made by sensor transducers associated with them.
- are able to make their identification, sensor measurements and other attributes available to external entities such as other objects or systems.
- can communicate with other Smart Objects.
- can make decisions about themselves and their interactions with external entities.

Objects such as consumer goods, product parts, assembly machinery, logistics and transportation items (e.g. pallets, containers, vehicles), warehouses, retailers' facilities or end-user assets are eligible for condition monitoring and can provide valuable information for themselves or other objects in their vicinity. In order to monitor their condition, we make use of embedded devices with wireless communication capabilities. These devices would be attached to the objects, becoming a part of them, the same way a bar-code sticker is part of the vast majority of today's products.



(a) (b)

Fig. 1. Smart Object system architecture (a) and implementation (b)

The devices attached to the objects are meant to provide a global identification, to sense the status of the object and/or their surroundings and to hold a wireless interface for data communication. These devices are thus aligned with the developments on sensor-enabled active tags, with the fundamental difference that our devices (which we call simply "nodes") hold the logic to not only communicate with each other, but to form ad-hoc networks for the better management of resources and data capture. Our nodes are basically WSN devices with a standardized unique identification. However, unlike traditional WSN, nodes are expected to move together with the objects they monitor and continuously interact with other nodes. This dynamism is not a common characteristic of such restricted devices and coping with it constitutes a big part of our work in this area.

Figure 1(a) provides an overall view of the architecture design for our vision of the Smart Object framework. The remaining of this section describes the two main components of this architecture: the SO networks and the Information Infrastructure.

B. Networking for management and information capture

RFID and sensor technologies that capture data about specific objects have traditionally used point to point communication between the device representing the object (e.g RFID tag) and the data reader (e.g RFID reader). This form of communication is sufficient for simple applications, but might be insufficient when large numbers of devices coexist or a certain degree of intelligence on the data gathering is required.

Smart Object networks utilize clustering for power management. Clustering extends the network lifetime by electing a representative network member, or Cluster Head (CH), which collects all the communication within the network and forwards it to the outside. Cluster heads are beneficial because they handle the burden of communicating with external entities, a task that is usually more power-intensive than intranetwork communication. Furthermore, CHs can provide a centralized control over network functionalities when needed. They may also be elected according to their particular capabilities, such as radio ranges, processing power, etc. On the downside, CHs consume more energy that the other network members and their role must be periodically rotated in order to avoid the premature exhaustion of their battery power. SO networks use the residual energy of a node (i.e the amount of power left in its battery to enable its operation) to calculate the best candidate when the CH role is rotated. This strategy yields the optimum energy balance among the network members when combined with other variables such as the number of network members. Networking of SO is also employed as a filter to data capture: rather than forming networks with random objects, SO may only interact with one another if they share a common context (e.g. participate in the same shipment, are parts of the same composite object, are stored in the same place). To achieve this, logical identification numbers and algorithms for classifying and prioritizing SO interactions are also included within the logic of the nodes.

An important challenge arising in dynamic, distributed wireless communication is the handling of unexpected network changes. Traditional WSN research has focused on data routing and resource management on static systems. However, the dynamic nature of SO interactions departs from existing WSN research and requires additional consideration to be embedded into the network protocols. As a part of the research in Smart Object systems, mechanisms to handle spontaneous additions and departures of SO to/from the network were developed. These mechanisms include a new addressing and routing protocol and several algorithms to handle data packets exchanged among Smart Objects.

For details that prove the energy efficiency of the proposed SO architecture, as well as a comprehensive discussion on the design of the classification and priority processes and dynamic considerations, please refer to [6]

C. Infrastructure for data sharing

A Smart Object itself is not enough to achieve the expected benefits of "smart products". There is also a need for flexible and efficient ways of managing the Smart Object information and making it available to end-users. This functionality is achieved by providing an Information Infrastructure with which Smart Objects can communicate.

The SO architecture presented here is event driven. For each change of the SO relationships on the network (e.g SO addition and removal, change of communication neighbors), an event is generated and propagated towards the Information Infrastructure. The infrastructure contains a repository of SO network structures, which is adjusted upon the reception of every event. By querying the repository, clients can acquire knowledge about the disposition of a Smart Object within its network and which condition it monitors. By analyzing this data, clients may not only subscribe to the real-time sensor information provided by a single SO, but may also determine which Smart Objects form part of the same contextual situation and retrieve their information with various degrees of granularity (ie. sensor, node, Smart Object or network). This functionality is provided through the Capture and Query Interfaces.

Architecture Implementation

The described architecture was implemented using Wireless Sensor Networks, Web Services and relational databases (Figure 1(b)). The resulting prototype provided a generic and flexible platform for testing a variety of scenarios . One such scenario, based on a supply chain application, is presented in the next section.

The implemented architecture is composed of two fundamental parts as described in section III: the Smart Object networks and the Information Infrastructure. Although not necessarily easier to develop, the Smart Object network constitutes a relatively simple physical architecture in which all the network members have an identical starting role where the interactions that occur during the network operation define the roles of the network members. Thus all the devices that form a Smart Object network are programmed with the same application, with the exception of the various sensor drivers

that are activated as needed. We chose the ANTS WSN platform [2] to implement the node functionality. The ANTS sensor nodes feature a 8 bit -controller, a 2.4Ghz transceiver, 128KB or Flash and 4KB of SRAM and a variety of sensor including pressure, humidity, temperature and accelerometer.

The SO network ((a) in figure 1(b)) communicates with the Information infrastructure via a gateway node (b). In the implementation, the gateway node serializes the SO events and transmits them to a Network Translator (c), whose role is to convert those messages into HTTP client requests to a Java Servlet server that acts as the gateway to the Information Infrastructure. The Information Infrastructure implementation architecture is more complex than the SO network since it involves many starting roles. XML-based Web Services (WS) were chosen due to their ability to provide cross-platform and cross-language communications over a network. Figure 1(b) details the software components and transport protocols that were used in the implementation of the information infrastructure. All the software was written in Java. XML and XSD were used to encode the events and event data. WSDL was used to describe the capture (d) and query interfaces (e). SOAP and HTTP were used as messaging protocols to transfer the XML-encoded events between the different architecture components. A PostgresSQL database was used as a repository (f) in order to store the structure of the Smart Object networks. Due to the flexible and interoperable nature of the XML-based WS, infrastructure clients could use a variety of methods for encoding requests sent to the Capture and Query Interfaces. In our implementation architecture, both Web Browser (h) and Java based clients (g) were built.

Example Scenario

We choose a Supply Chain scenario to illustrate the Smart Object framework, architecture and prototype presented in sections III and IV. Consider a package (e.g. a pallet) containing a batch of refrigerated products. The contents of this pallet are produced at the manufacturer, packaged and sent to wholesalers and retailers. Along this process, the pallet is stored in several warehouses, and is transported over land by a fleet of refrigerated trucks that belong to various logistics and cargo companies. Each pallet is equipped with a node that can sense ambient temperature. Furthermore, the trucks incorporate temperature and humidity sensors. Figure 2 depicts the described scenario for two pallets and one truck. Note that this scenario is easily extensible, not only for additional pallets or trucks, but also for more complex Smart Object networks (e.g where each box in each pallet carries a node) and additional logistic players (e.g. warehouses, other transport mechanisms, etc).

Let's assume that the node situated on the refrigerated truck storage cabin has access to the Internet through some mobile gateway (e.g. cellular network or satellite). A system implementation based on Smart Objects supports the following unique features.

A. Real-Time Condition Tracking

The condition of the pallets, result of the interpretation of sensor measurements taken by their integrated tags, can be tracked in real-time along their entire supply chain. The tracking is independent of the location of the client, the truck and the pallets as long as the identification of the pallets is known and their network CH has access to a gateway

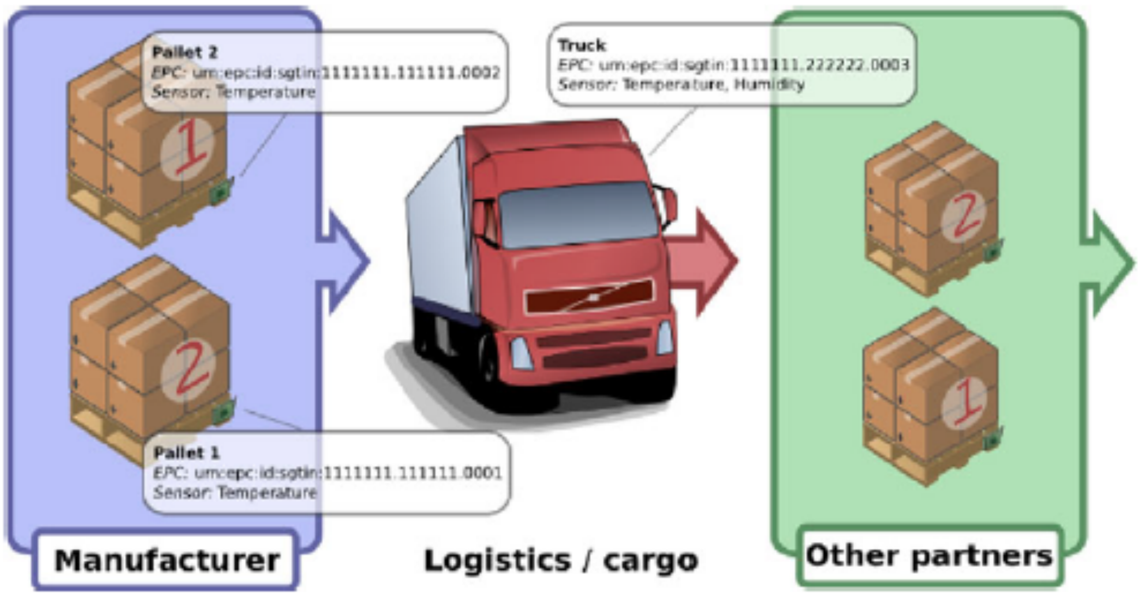


Fig. 2. Example Scenario for condition monitoring of refrigerated products in the Supply Chain

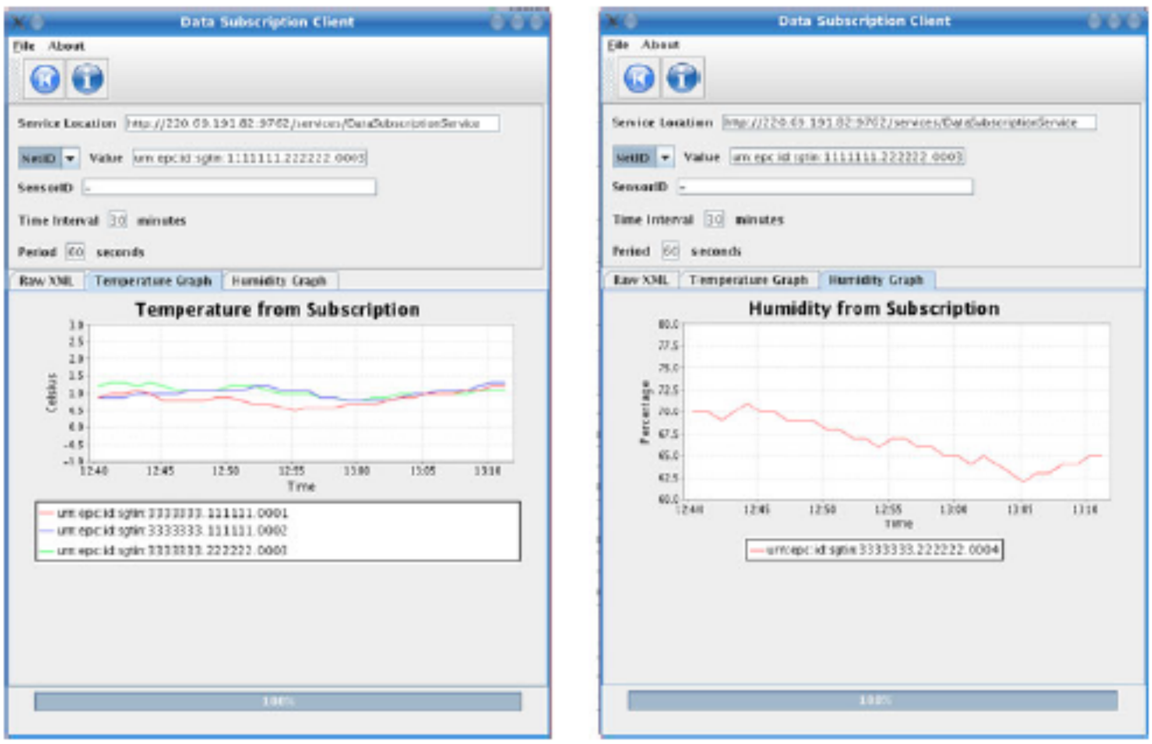


Fig. 3. Data subscription Web Service Java client software running the example scenario

connected to the Internet. Partners such as the manufacturers that released the product, retailers that are waiting for their shipment or the logistic companies that are in charge of the transportation of the goods can enable this tracking by just subscribing to the capture interface with the identification numbers of the pallets (EPCs in this example).

B. *Contextual Monitoring*

The SO networking design makes possible to discover additional sensor sources relevant to the context of a particular monitored item. By querying the infrastructure repository with the EPC of the pallet, the retailer can retrieve the EPCs of all the SO participating in its network. Using this mechanism, the retailer could determine that the truck contains a humidity sensor relevant to the condition of the refrigerated product, and subscribe also to that stream of data. Finally, by leveraging the EPC Network standards and infrastructure, it is possible to query on-line databases and obtain additional information about specific Smart Objects. For example, if sensor hardware metadata were made available though the information services of the manufacturer or logistics companies (http://www.epcglobalinc.org/standards/epcis), a trading partner in the example could determine the accuracy of both truck and pallet temperature sensors and choose which values to use.

C. *Configuration Flexibility*

The SO architecture design permits the assignation of priorities and restrictions to the way the SO interact. In this way, logistic companies could ensure that only products from their selected suppliers make use of the resources of the company (e.g only pallets that have the right identifiers can use the truck's sensor and gateway). Additionally, should each item on a pallet carry a node, pallet networks would be formed prior to the truck network, building an effective hierarchical network structure aiding to the discovery of meaningful contextual condition information.

Figure 3 shows a screenshot of the Data Subscription client software, monitoring all the sensor sources from the SO network formed inside the truck from the example scenario, for a period of 30 minutes, in 60 second intervals.

Challenges

I. *Economic challenges*

It is only in recent years that simple passive RFID tags have become available at sufficiently affordable prices (around 7c per tag in large volumes) that many industry sectors are considering widespread adoption of RFID. Sensor-enabled active tags are likely to cost considerably more than simple passive RFID tags because of the additional cost of the sensor, memory capacity and batteries. For this reason, many of the early trials apply them to reusable assets (e.g food trays, pallets) rather than individual items in order to amortize the cost over a much longer period of service.

II. *Security and trust issues*

RFID usually requires the assignment of unique identifiers for each object. This results in fine-grained visibility and tracking information, but means that an individual object is no longer 'anonymous' as simply another instance of a particular product type. At the same time, complete sensor information for an object is realistically likely to be fragmented and distributed across its lifecycle, with each organization holding only the sensor information that was collected while the object was within their custody. In order to gather complete sensor information from across multiple organizations , it may be necessary to provide authentication and business relationship credentials in order to justify the request, both for querying data from the Smart Objects and when they attempt to connect to the infrastructure gateways.

III. *Scalability challenges*

A further challenge to the collection of sensor data is the capacity available for storage of historical data. Consideration should be given to mechanisms that allow thresholds and also more complex exception criteria to be defined in a standardized manner. This may ultimately lead to a different paradigm for information sharing, in which alerts and details of exceptions are returned by queries, rather than large volumes of low-level location and sensor data. This strategy may allow compression of historical data for long term storage and could also address some of the data sharing concerns since organizations may prefer to provide object information only when exceptions and alerts arise.

Conclusion

We have presented an architecture that uses Smart Objects to integrate technologies such as automatic identification, sensor systems, embedded processing, context-aware ad-hoc networking and Internet-based services, which are identified as central to the realization of the IoT concept. Practical experience gained with the implementation demonstrates that it is both feasible and flexible to adapt to a variety of applications and off-the-shelf technologies. However, a number of identified challenges suggest that the adoption of the IoT in general, and our architecture in particular, is not only limited by developments in technology but also by social and trust issues.

Our research has opened up several opportunities for new applications and research areas that we would like to investigate in the future. We will explore how to make the Smart Objects first-class citizens on the IoT without the need of translation gateways, aiming to make the “things” real players in the Internet. We will also focus on higher integration with existing standards such as the EPC Network architecture, OGC SWE or the IEEE 1451. Finally, we will investigate mechanisms for adding top-down functionality to our architecture, allowing functionalities such as the processing of downstream commands such as actuation, which would depend on the capability description of the objects.

References

[1} EPCglobal Inc, The EPCglobal Architecture Framework, Standard Specification, September 2007
[2] D. Kim, T. Sanchez Lopez, S. Yoo, J. Sung, ANTS: An Evolvable Network of Tiny Sensors ,Embedded and Ubiquitous Computing, LNCS, Springer, 3824/2005, 142-151
[3] PROMISE FP6 - 507100, Product Lifecycle Management and Information Tracking using Smart Embedded Systems - PROMISE, The PROMISE Consortium, EU, 2005
[4] Open Geospatial Consortium Inc. OGC Sensor Web Enablement: Overview and high level architecture, OGC White Paper, OGC 07-165, v3, December 2007
[5] The BRIDGE Consortium, BRIDGE: Building Radio Frequency Identification Solutions for the global environment, October 2006
[6] T. Sanchez Lopez, D. Kim, G. Huerta Canepa, K. Koumadi, Integrating Wireless Sensors and RFID Tags into Energy-Efficient and Dynamic Context Networks, The Computer Journal 2008; doi: 10.1093/comjnl/bxn036
[7] J. Sung, T. Sanchez Lopez, and D. Kim, The EPC Sensor Network for RFID and WSN Integration Infrastructure PerComW 2007, IEEE Computer Society, 2007, 618-621
[8] K. Finkenzeller. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, Wiley 2003
[9] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless Sensor Networks: a survey, Computer Networks, Elsevier, 2002, 38, 393-422
[10] A.P. Sample, D.J Yeager, P.S. Powledge, J.S. Smith, Design of a Passively-Powered, Programmable Sensing Platform for UHF RFID Systems, Proceedings of IEEE International Conference on RFID, IEEE Computer Society, 2007, 149-156
[11] J. Cho, Y. Shim, T. Kwon, Y. Choi, SARIF: A novel framework for integrating wireless sensors and RFID networks, IEEE Wireless Communications, 2007, 14, 50-56
[12] M-J. Franklin, S-R. Jeery, S. Krishnamurthy, F. Reiss, S. Rizvi, E. Wu, O. Cooper, A. Edakkunni, W. Hong Design Considerations for High Fan- In Systems: The HiFi Approach, Proceeding of the CIDR 2005, VLDB Endowment, 2005, 290-304
[13] K. Aberer, M. Hauswirth, A. Salehi, Global Sensor Networks, Technical report LSIR-REPORT-2006-001

[14] AUTOIDLABS-WP-SWNET-018 (2007) Architecture Development for Sensor Integration in the EPCglobal Network, AutoID-Labs, 2007
[15] Floerkemeier. C, Langheinrich. M, Fleisch. E, Mattern. F, Sarma. S, Preface of the Proceedings of the The Internet of Things 2008, LNCS, Springer, 4952/2008, V-VI

Tomás Sánchez López is a Research Associate at the Distribution Information and Automation Laboratory, University of Cambridge. His research interests focus on how to provide sensor functionalities within the current RFID standards and information architectures. Sanchez Lopez has a Ph.D in Computer Science from KAIST, South Korea, and is actively involved in the activities of the Auto-ID lab Cambridge. Contact him at tsl26@cam.ac.uk **Damith C. Ranasinghe** is the associate director of the Auto-ID Lab at the University of Adelaide. His research interests are on RFID and sensor data management, lightweight security and agent based systems Ranasinghe has a PhD from the University of Adelaide, Australia. Contact him at damith@eleceng.adelaide.edu.au.

Mark Harrison is the director the Auto-ID Lab at the University of Cambridge. His research interests include the design of information services and lookup systems for networked RFID, as well as enhanced trace and trace systems. He is also actively involved in standards development at EPCglobal. He has a PhD in Physics from the University of Cambridge. Contact him at mark.harrison@cantab.net

Duncan McFarlane is Professor of Service and Support Engineering at the Cambridge University Engineering Department, and head of the Centre for Distributed Informational and Automation Laboratory . His research work is focused in the areas of distributed industrial automation, reconfigurable systems, RFID integration and the role of automation and information solutions in supporting service environments. Contact him at dcm@eng.cam.ac.uk