Daniel Giusto
Antonio Iera
Giacomo Morabito
Luigi Atzori
Editors

The Internet of Things

20th Tyrrhenian Workshop on Digital Communications

The Internet of Things

Daniel Giusto · Antonio Iera · Giacomo Morabito
Luigi Atzori

Editors

The Internet of Things

20th Tyrrhenian Workshop
on Digital Communications

Editors
Daniel Giusto
Università di Cagliari
Dipto. Ingegneria Elettrica e
Elettronica
Piazza d' Armi
09123 Cagliari
Italy
ddgiusto@diee.unica.it

Antonio Iera
Università Mediterranea
Fac. Ingegneria
Dipto. D.I.M.E.T
Via Graziella (Feo di Vito)
89100 Reggio Calabria
Italy

Giacomo Morabito
Università Catania
Dipto. Ingegneria Elettrica
Elettronica e dei Sistemi (DIEES)
Viale Andrea Doria, 6
95125 Catania
Italy

Luigi Atzori
Università di Cagliari
Dipto. Ingegneria Elettrica e
Elettronica
Plazza d' Armi
09123 Cagliari
Italy

Printed on acid-free paper

Preface

In the last few years, a stimulating idea is fast emerging in the wireless scenario: the pervasive presence around us of a variety of "things" or "objects", such as RFID, sensors, actuators, mobile phones, which, through unique addressing schemes, are able to interact with each other and cooperate with their neighboring "smart" components to reach common goals.

This novel paradigm, named "The Internet of Things" (IoT) continues on the path set by the concept of smart environments and paves the way to the deployment of numerous applications with a significant impact on many fields of future every-day life. In this context, logistics, Intelligent Transportation Systems (ITS), business/process management, assisted living, and e-health are only a few examples of possible application fields in which this novel paradigm will play a leading role in the next future.

Actually, many challenging issues still need to be addressed and both technological and social nodes untied before the IoT idea being widely accepted. Central issues are making a full interoperability of such devices possible, enabling their adaptation and autonomous behavior, as well as guaranteeing trust, privacy, and security. Also, the IoT idea poses several new problems concerning the networking aspects. In fact, the "things" composing the IoT will be characterized by low resources in terms of both computation and energy capacity. Accordingly, the proposed solutions need to pay special attention to resource efficiency besides the obvious scalability problems.

The papers included in this volume present a picture of the current state of the art on the above issues; more specifically, concepts and ideas are discussed on networking, middleware, security and privacy, RFID and sensor networks, as well as electromagnetic aspects.

1 Networking Issues in the IoT

Networking issues are of great relevance in the IoT scenario, especially when sensed data and control commands need to be routed through different networks of objects or have to be delivered to servers in the Internet. Routing and addressing are two of the main issues, which need to be addressed taking into account the fact that

the network topologies (physical and logical) vary over the time so that different gateways and clusters of mobile nodes are used to transmit from one network to another. A common scenario analyzed by Bernardo Leal and Luigi Atzori in "*Objects Communication Behavior on Multi-Homed Hybrid Ad Hoc Networks*" is one of the Mobile Ad hoc NETworks (MANETs) interconnected to the fixed networks by means of different gateways. Such multi-homed MANETs can be seen as an extension to the existing infrastructure. Accordingly, MANET nodes may seamlessly communicate with those on the fixed network forwarding packets through appropriate gateways. Two of the aspects that may affect the performance are node address allocation and dynamic gateway changes. When objects in MANETs move around, they may find themselves on a different sub network from the one they have registered in and got their address from. For that reason, their IP address must be changed accordingly while ongoing connections must be maintained and the packets belonging to these connections must be delivered continuously. A crucial role in this context is that of the routing protocols, which may be either proactive, such as the OLSR (Optimized Link State Routing Protocol), or reactive, like the AODV (Ad-hoc On-Demand Distance Vector). The selection of one of these two approaches and the configuration of the adopted protocol is a big issue that needs to be evaluated depending on the type of communications and the main performance issues.

Another emerging solution proposed in the paper entitled "*Traffic Classification in the Presence of Routing Asymmetry*", authored by Manuel Crotti, Francesco Gringoli, and Luca Salgarelli, is that based on the adoption of asymmetric routing, which is a practice already common in the Internet core and is going to affect parts of the network that are closer and closer to the edges, such as the IoT networks. In order to maintain their effectiveness in this environment, appropriate traffic analysis techniques need to be made robust to the effects of asymmetric routing. Performance evaluation of routing protocols in WSNs is presented by L. Bergesio, M. Franceschinis, M. Spirito, and R. Tomasi in their paper. They specifically focus on a multi-hop routing solution, called *Hopefully Longest Jump First*, specifically proposed for WSNs arranged in a linear topology. This solution is compared with two simple approaches, named *Single Hop* and *Limited Flooder*. At the application level, a Master Node has been implemented at one side of the WSN, which progressively queries each of the N Slave Nodes. On its turn, when queried, a Slave Node replies to the Master Node. The analysis is based on performance metrics like end-to-end delay and end-to-end packet delivery success rate, also considering the impact of the distance between two adjacent nodes and thus the expected number of neighbors within a node radio coverage.

Medium access control and management continues to be a subject extensively investigated within the IoT arena, since it heavily affects the communication performance in terms of delays, losses, throughput, and reliability. When devising new strategies, it is important to focus on the self-managing, self-configuring, and self-regulating features, especially if the resulting network has to operate in emergency areas as in the case of the management of catastrophes. In this context, an important issue addressed by Emanuele Cipollone, Francesca Cuomo, and Anna Abbagnale in the paper "*A Distributed Procedure for IEEE 802.15.4 PAN Coordinator Election*

in Emergency Scenarios" is the selection of the network coordinator which has to be performed by also taking into account energy saving during data delivery, thus increasing the network lifetime in case of battery supplied devices (e.g., in case of Wireless Sensor Networks – WSNs) and delivery delay reduction. Cooperation between wireless networks has also quickly gained the interest of many researchers since several studies have shown how the performance can be improved by using principles of cooperation. In particular, a novel architecture, namely Cellular Controlled Peer-to-Peer (CCP2P), has been introduced in the last years. According to it, cellular devices can create cooperative clusters with neighboring devices in their proximity using a short range technology. Each terminal is then contributing to the cooperative cluster by sharing its cellular link. The grouped members acting in a cooperative manner can achieve better performance than a standalone device, in different scenarios. This is the context studied by Emanuele Scuderi, Rocco Parrinello, David Izal, Gian Paolo Perrucci, Frank Fitzek, Sergio Palazzo, and Antonella Molinaro in "*A Mobile Platform for Measurements in Dynamic Topology Wireless Networks*".

However, still great efforts are needed to make the cooperation effective and reliable in realistic scenarios where the peers are continuously moving and the channel is disturbed by concurrent communications in the same geographical area. Whereas cooperation can improve the performance in terms of energy consumption, broadcast techniques allow for reaching the widest area in the shortest possible time which is a feature highly demanded in case of emergency transmission. This is the case of safety-related applications in self-organizing Vehicular Ad-hoc NETwork (VANET), where vehicles share and distribute information by rebroadcasting a received information packet to their neighbors. An efficient broadcast technique can offer a high reactivity without sacrificing the communication reliability. In this context, Cluster-based Irresponsible Forwarding (CIF) is a novel broadcast multi-hop forwarding protocol introduced in "*Cluster-based Irresponsible Forwarding*" by Stefano Busanelli, Gianluigi Ferrari, and Sooksan Panichpapiboon. CIF integrates the recently proposed IF probabilistic forwarding approach with a loosely structured clustered architecture. The clusters of vehicles that naturally form in VANET are typically "ephemeral" and tend to be a source of network congestion, that penalize the performance of "pure" probabilistic approaches. CIF attempts to recognize the presence of ephemeral clusters and adapts its forwarding strategy to the underlaying instantaneous network topology. Also the paper "*Dynamic Spectrum Access Communications: Wavelet Modulation with Unequal Power Allocation*", by Marco Lixia and Maurizio Murroni, addresses network access layer issues by proposing an optimization in the power allocation when using the available spectrum in a dynamic way. An adaptive Wavelet Modulation (WM) scheme is proposed to exploit available resources of the channel while avoiding interferences with the primary users of the spectrum. The power is distributed according to both the sensitivity to channel errors and channel availability. Genetic Algorithms are used to optimize weights with the constraint of average energy per bit remaining unaffected.

Flow control is another crucial issue in heterogonous wireless networks used in the IoT scenario, especially when dealing with multimedia communications.

The paper authored by Enzo Baccarelli, Mauro Biagi, Nicola Cordeschi, Tatiana Patriarca, and Valentina Polli, "*Optimal Cross-Layer Flow-Control for Wireless Maximum-Throughput Delivery of VBR Media Contents*", focuses on the design of control policies and proposes an approach based on the maximization of the average throughput over the wireless last-hop, under constraints on the maximum connection bandwidth allowed at the Application (APP) layer, the queue-capacity available at the Data-Link (DL) layer, and the average and peak transmit energies sustained by the Physical (PHY) layer. The resulting controller is rate-based and operates in a cross-layer fashion that involves the APP, DL, and PHY layers of the underlying protocol stack.

Finally, the paper "*A Secure MPLS VPN Infrastructure for Complex Geodata Sensor Network*", by Mirko Luca Lobina and Tatiana Onali, studies the issues of interconnecting geodata sensor networks when deployed to monitor environmental factor in an extended geographical area. The use of the MPLS protocol is considered in this context, with a keen attention to issues related to the bandwidth management and security, when short messages are transmitted through the backbone network.

2   Middleware for the Internet of Things

The availability of a middleware layer hiding the details of different technologies is fundamental to exempt the programmer from details that are not directly pertinent to her/his focus, which is the development of the specific application enabled by the IoT infrastructures. The IoT may benefit a lot from the existence of such a middleware, since new services will be easily developed and objects interaction will be strongly enhanced. This is a software layer interposed between the technological and the application sub-levels. Several solutions are under study. The WhereX solution, introduced by Antonio Puliafito, Angelo Cucinotta, Antonino Longo Minnolo, and Angelo Zaia in "*Making the Internet of Things a Reality: The WhereX Solution*" has been developed responding to SOA (Service Oriented Architecture) and Multichannel Communication technologies. The use of the SOA principles provides the highest level of flexibility and scalability to the system in the organization of both the external integration processes and the exchange processes within the middleware, by favoring the addition/modification of functions and services (scalability). The use of the XMPP communication model is very important because, since this is a real-time communication protocol, it can provide a high level of interactivity and can simplify the integration with enterprise applications. The SAI (Service Application Integration) middleware solution described in "*A Scalable Grid and Service-Oriented Middleware for Distributed Heterogeneous Data and System Integration in Context-Awareness Oriented Domains*" by David Parlanti, Federica Paganelli, and Dino Giuli, is also based on the adoption of a SOA approach for easing the integration of heterogeneous resources for the development of context-aware applications in enterprise domains. The SOA approach interprets distributed systems mainly as a problem of service

specification, implementation, and composition. A "service" may be defined as a computational entity endowed with an open and addressable specification of its expected behavior. The definition of the "computation entity" is then extended to include software components encapsulating sensors/actuators functionalities. Integration of such real-world devices and business systems usually requires decoupling between service consumers and providers, thus demanding support also for one-way, notification-response, and solicit-response interaction patterns. To address such invocation requirements, SOA's implementation solutions should also be correlated with "message-oriented" approaches. Message orientation gives new insights on service provision/consumption as well as on the overall SOA architectural style. The InterDataNet architecture is another middleware solution proposed by Franco Pirri, Maria Chiara Pettenati, Samuele Innocenti, Davide Chini, and Lucia Ciofi in "*InterDataNet: A Scalable Middleware Infrastructure for Smart Data Integration*". InterDataNet is based on the SOA principles too. It is designed to enable heterogeneous objects networks to expose and integrate their smart data. At the core of the system sits the InterDataNet middleware that defines an object Information Model and the related Service Architecture operating on it in order to provide: a scalable and open service to support a consistent reuse of objects identifiers, that is a global reference and addressing mechanism for locating and retrieving objects in a Web-wide scale; a set of transparent application-services functions, namely historic data management and replica management.

The management of the Resource Identifiers of the Real World Objects (RWOs) is the main subject of the CONVERGENCE middleware framework proposed by Nicola Blefari Melazzi in "*CONVERGENCE: Extending the Media Concept to Include Representations of Real World Objects*". CONVERGENCE is aimed at enhancing current media handling with new functionality and extend the traditional concept of media to include digital representations of RWOs. The Convergence framework is based on the concept of Versatile Digital Item (VDI), a structured package of digital content and meta-information, inspired by the MPEG-21 standard, but designed to address a broader range of application domains, including the management of RWOs in the Internet of Things. The VDI is supported by an innovative middleware and by tools and applications. This framework incorporates six innovations: (1) VDIs provide uniform mechanisms to handle different classes of information, including Real World Objects; (2) VDIs are intrinsically dynamic, allowing both providers and consumers to update content; (3) VDIs support "digital forgetting" (automatic "un-publishing", automated garbage collection of VDIs after a user-defined expiry date); (4) VDIs meet security and privacy needs of both professional and non-professional consumers and providers; (5) VDIs support new modes of semantic search; (6) VDIs allow easy sharing of information across multiple, heterogeneous devices.

Particular attention has to be devoted to the middleware solutions that specifically deal with the management of emergency situations. In this scenario, addressed by Fabrizio Ronci and Marco Listanti in "*Service Oriented Middleware Solutions for Emergency Communication Networks*", a number of operators, decision-makers, and institutional and commercial service providers are usually supposed

to cooperate in order to assist involved population and environment, to overcome the crisis and to start reconstruction. As far as conventional, and possibly inadequate, communication services, basically relying on radio voice calls, yield to a wide gamut of real time, interactive and multimedia data oriented information flows, new viewpoints on network architectures arise from integrating available information, communication and media technologies. All these network resources and components, including today's mobile devices that, as for performance, are a lot more powerful than those of the early days, are able to host very sophisticated and versatile software. This fact enables the usage and exploitation of middleware solutions to integrate knowledge, but also to enhance reliability, to provide transparency, and to guarantee scalability in respect of physical, link, routing and transport technologies, and schemes.

3   Localization and Applications

As we already said, the IoT concept has the potential to change radically our life, thanks to innovative smart applications that adapt their behavior according to the specific context. One of the most important context parameters is the position of individuals or objects. Indeed, several applications can be thought that involve the localization and tracking of people, assets, or goods.

In the past, a large effort has been devoted to the problem of localization of communication nodes. However, the existing results cannot be applied *tout cour* to the IoT scenarios given that nodes have much lower processing and communication resources. Therefore, new methodologies must be devised with higher localization accuracy and higher efficiency.

To answer this research need, several approaches are possible. In this volume, there are two papers that cover the most relevant of such approaches: the use of the electromagnetic signal and the use of the acoustic signal.

More specifically, in "*Localization Issues in a ZigBee based Internet of Things Scenario*", Ugo Biader Ceipidor, Massimiliano Dibitonto, Luca D'Ascenzo, and Carlo Maria Medaglia propose a methodology that uses fixed network devices as reference points. In fact, the RSSI between mobile nodes that need to be localized and the above reference points is measured to obtain distance values and therefore, to derive localization information.

Instead, in the paper entitled "*Low-Complexity Audio Signal Processing for Localization in Indoor Scenarios*", Marco Martalò and Gianluigi Ferrari propose an innovative approach that allows to perform low complexity localization based on the audio signal. More specifically, the proposed methodology allows to localize entities that emit sound through special devices called *anchors*. Based on such an approach, both a centralized and a distributed solution have been designed. Matlab simulations show that the proposed approach allows to achieve high localization accuracy with low processing load. As a future work, authors aim to solve the localization ambiguities raising in certain special cases.

Localization is one of the objectives pursued by Stefano Tennina, Luigi Pomante, Fabio Graziosi, Marco Di Renzo, Roberto Alesii, and Fortunato Santucci in "*Integrated GPS-denied Localization, Tracking, and Personal Identification*". In that paper, a solution is presented that utilizes a biometric badge implementing positioning/tracking algorithms as well as authentication procedures based on fingerprinting matching. Such solutions can be utilized to enable or deny access to restricted areas, for example, to localize patients in hospitals. Localization and tracking are achieved by means of a novel distributed algorithm called ESD (*Enhanced Steepest Descent*). Experimental results show that ESD achieves localization accuracy comparable to the leading solutions much more rapidly.

In certain application scenarios, exact identification and localization of individuals is not necessary, it is sufficient to have information about the number of persons in a certain area and the gender distribution (i.e., how many women? How many men?). Accordingly, in "*Design and Implementation of Smartphone Applications for Speaker Count and Gender Recognition*", Alessio Agneessens, Igor Bisio, Fabio Lavagetto, and Mario Marchese propose a methodology that allows to obtain such information utilizing smart-phones. Current realization of such methodologies allows to distinguish one speaker cases from two speaker cases; however, extension to the case in which several speakers can be distinguished are possible in the future. Prototypes of the proposed methodologies have been implemented on communication devices based on Symbian OS. Experimental results assess the accuracy of the proposed scheme.

In other application scenarios, presence of individuals in a certain area can be identified by means of cameras. In the IoT scenarios, it is of paramount importance to achieve high compression gain given the limitations in the capacity of the devices. Accordingly, in the paper "*Video Coding and Motion Estimation at the Decoder*", Claudia Tonoli, Pierangelo Migliorati, and Riccardo Leonardi present a methodology that achieves high compression ratio thanks to effective and efficient motion estimation at the decoder side. The methodology is based on the Last Square Estimation (LSE) prediction and achieves good performance as demonstrated by experimental results.

Observe that the transmission of video information has strict QoS requirements. Support of such requirements is important especially in the case of disaster recovery applications. Accordingly, there is the need for appropriate QoS management solutions such as the one proposed in "*Inter-Vehicle Communication QoS Management for Disaster Recovery*" by Paolo Orefice, Luigi Paura, and Amedeo Scarpiello. In that paper, focus is on inter-vehicle communications where several problems arise given the dynamics of network topology and link characteristics. Interesting feature of the proposed solution is that it can easily manage new access technologies as they become available in the application scenario without the need of upgrades of the management procedure. Preliminary performance results show that the proposed approach works correctly in PropsimC2 emulator.

4   RFID and Sensor Networks Technologies

For what concerns RFID and sensor networks, it shall be recognized that both of them play a special role within the "Internet of Things" paradigm. According to the International Telecommunication Unit (ITU Report 2005), Internet of Things can be defined as a vision "*. . . to connect everyday objects and devices to large databases and networks. . . (using) a simple, unobtrusive and cost-effective system of item identification. . .*".

Therefore, according to the IoT vision, smart sensor/actuators need to be enhanced with connection capability to locally available networks to the purpose of interacting with the real world. Through the exploitation of smart distributed "objects", such as for example sensors, actuators, RFID tag, and the implementation of data fusing and mining algorithms, the end-user is allowed to identify objects, access real time data, and undertake appropriate actuation strategies, ubiquitously and via Internet.

This is the reason why the enhancements and the integration of communication potentials among RFID tags, sensors, and actuators are key issues to be addressed in any research/publication related to the IoT, together with the integration of the cited devices into hybrid wireless sensor networks.

Researches addressing the RFID and Sensor/Actuator related issues are manifold. Among them, FOSSTRAK (Free and Open Source Software for Track and Trace, an open source RFID software platform that implements the EPC Network specifications), CASAGRAS (Coordination And Support Action for Global RFID-related Activities and Standardization, a European Union-sponsored project looking at future standardization for RFID and especially RFID's role in the emerging Internet of Things), and EPoSS (European Technology Platform on Smart Systems Integration, an industry-driven policy initiative defining R&D and innovation needs as well as policy requirements related to Smart Systems Integration and integrated Micro- and Nanosystems) are examples that deserve a citation because part of their activities are preparatory to the future platforms integrating both technologies (RFID and Sensors) into single IoT platforms.

Ongoing researches testify to the fact that still the set of actions that the future objects should be able to do and the enhancements that are required to best integrate these objects into IoT frameworks is a matter of investigation. This is why in the present publication, some of the main issues relevant to both RFID and Sensor/Actuator networks will be introduced to the reader.

Aspects related to middleware-based solutions for RFID integrations are addressed within the specific session of the present publication dealing with middleware solutions for the IoT. Due to the relevance of the topic, more papers are dedicated to the RFID topic. Some of them deals with RFID technology in general, while the others more specifically address electromagnetic aspects related to the RFID technology. As a result, the reader will be able of obtaining an in-depth picture of main potentialities and limitations of the RFID technology, constraints and enabling technologies for its future evolutions, as well as its effectiveness in impacting in specific IoT application scenarios (e-health, ITS, Logistics, etc).

Since the reading of the first paper, "*Beyond the ID in RFID*" by Christian Floerkemeier, Rahul Bhattacharyya, and Sanjay Sarma, it clearly emerges that RFIDs are fast moving toward the implementation of functions going well beyond the mere identification. Battery powered wireless sensors are the most common commercial wireless sensors used today. However, limited battery life and higher costs limit their deployment in some sensing applications. For this reason, the authors analyze the advantages and shortcomings of alternative passive wireless sensing approaches by emphasizing an emerging paradigm of RFID tag antenna based sensing that offers great potential for the development of ultra low cost, long lasting wireless sensors. Authors conclude that the gains from adopting this sensing approach may outweigh the shortcomings.

A further performance study aiming at the characterization of passive ultra-high frequency (UHF) and radio frequency identification (RFID) tags is presented by Leena Ukkonen and Lauri Sydänheimo in their paper "*Performance Characterization of Passive UHF RFID Tags*". In this paper, the analyses of the effects of dipole antenna width and of the impedance matching properties of a bow-tie tag antenna are two characterization examples used to investigate the harvesting properties of the tag and the significance of the backscattered signal strength and radar cross section (RCS) of the tag.

Different RFID tag technologies and their main characteristics, design, and application are the subject of "*Chipless Tags, the Next RFID Frontier*", by S. Tedjini, E. Perret, V. Deepu, and M. Bernier, which focuses on the emerging concept of the so called "chip-less configurations". The interesting aspects of this tag family (also known as RF barcodes) lay in the fact that they do not use IC chip and the information is directly coded on the surface and/or in the volume of the structure; besides, they are very attractive in terms of cost and data security. The importance of having a clear picture of this novel technology is testified by the number of research projects worldwide dedicated to the development of efficient and versatile chipless tags and to the recent market projections showing that chipless tags will reach 60% of the RFID market before the end of the next decade.

Chip-less configuration is not the only possible enhancement to RFID. Also, the use of Ultrawide bandwidth (UWB) technology to enhance the RFID performance in specific IoT application fields, such as the accurate object localization, is a promising approach. UWB technology might allow next generation RFID systems to overcome most of the main limitations of current narrow bandwidth RFID technology, such as reduced area coverage, insufficient ranging resolution for accurate localization, low security, sensitivity to interference, and scarce multiple access capability. The paper "*Backscatter Communication using Ultrawide Bandwidth Signals for RFID Applications*", by F. Guidi, D. Dardari, C. Roblin, and A. Sibille aims at contributing to this issue, shows that it is possible to provide both identification and high-definition localization of objects by applying the UWB technology to (semi-) passive RFID based on backscatter modulation.

Passive RFIDs are the subjects of the paper "*Passive RFID Integrated Transponders for Automotive Applications*", by Alberto Toccafondi, Cristian Della Giovampaola, Paolo Braconi, and Alessio Cucini. In this paper, the authors specifically

stress the effectiveness of the RFID technology in future IoT scenarios (envisaged for Intelligent Transportation Systems), where the objective is the identification of moving vehicles within a mono-lane scenario for non-stop road-toll operation. To this aim, they propose and analyze a reference system using a HF-UHF RFID integrated transponder. Numerical simulations and experimental results conduced on a transponder prototype confirm the possibility of using this technology for the intended objective.

A different application field in which the IoT paradigm will surely play a starring role in the near future is the one in which the paper "*Sensor-Oriented Passive RFID*" by Gaetano Marrocco, Cecilia Occhiuzzi, and Francesco Amato is conceived. In fact, it is particularly focused on the monitoring of human body features, even if the proposed ideas and devices may also be applied in a variety of different scenarios. More specifically, the paper starts from the consideration that designing low-cost antennas for sensing applications is still a great challenge, especially when the human body is involved. In this view, the authors address the design of new UHF tag antennas for sensing applications able to host detectors and additional electronics but also to act as passive sensors themselves for some modification of the target.

Pharmaceutical distribution is a further sample scenario in which item-level tagging is one of the main challenges in order to improve track and trace systems. The paper "*Performance Evaluation of UHF RFID tags in the Pharmaceutical Supply Chain*", by M. De Blasi, V. Mighali, L. Patrono, and M. L. Stefanizzi, introduces a performance comparison between near field and far field UHF RFID systems. The final conclusion of this work is that the use of passive far field UHF tags could represent the de-facto solution for item-level tracing systems in the whole supply chain. Furthermore, the obtained results lead the authors to assert that the same solution can be easily extended to other sectors in which the item-level traceability is still an important aspect.

Finally, interesting contributions concerned with the business value of RFID technology in future logistics scenarios are the topic of paper "*The Benefits of RFID and EPC in the Supply Chain: Lessons from an Italian Pilot Study*", by Massimo Bertolini, Eleonora Bottani, Antonio Rizzi, Andrea Volpi and paper "*RFID Data Analytics in Apparel Retail*", by Frédéric Thiesse and Jasser Al-Kassab.

In the first one, the potential benefits of RFID technology and EPC Network on the overall fast moving consumer goods (FMCG) supply chain are quantified. The authors show that the largest part of the RFID benefits can be achieved through collaboration between multiple supply chain players. Examples of such benefits include: automation of supply chain processes, better inventory management and decrease in safety stocks, streamlining of other processes, and increase in turnover. While, in the second paper, the interesting contribution of Frédéric Thiesse and Jasser Al-Kassab deals with the business value of large amounts of data generated by RFID data collection infrastructures. The focus of the authors is on a recorded trace data derived from a department store that implemented RFID in its menswear department to seamlessly track thousands of items on their way from the distribution center to the point of sale. The output of their case study indicates that RFID poses an untapped opportunity for retail companies to improve category management,

store layout design, inventory control, and process execution, assumed that the company's individual capabilities exist to translate RFID data into value.

Besides RFID, also the "Sensors" issue is addressed in the present publication from the specific perspective of the Internet of Things. By this meaning, wireless sensors are seen like a companion technology of RFID, in the view of the deployment of common *IoT* infrastructures including RFID and Sensors. Therefore, in this publication the followed approach has been twofold: first novel models of sensor networks are addressed and studied in a couple of papers and then novel applications of Sensor and Actuator networks in very appealing scenarios are introduced as further contributions

Olivier Alphand, Andrzej Duda, Martin Heusse, Benoit Ponsard, Franck Rousseau, and Fabrice Theoleyre, contribute to the present publication with an interesting position paper, "*Towards the Future Internet of Sensors*", in which they propose a new view on the integration of wireless Sensor and Actuator Networks (SAN) in the Internet. According to their approach, the network conveys typed data chunks while applications organize communication according to the Publish/Subscribe model: data consumers subscribe to chunks advertized by producers. The main element of the proposed model is a data router device interconnecting different wireless SAN and offering a data centric view on the physical world to the rest of the Internet.

Still novel models of Sensor Networks (termed "refining" and "expanding") and related issues are the subject of the paper "*Energy and Distortion Minimization in 'Refining' and 'Expanding' Sensor Networks*" by Franco Davoli, Mario Marchese, and Maurizio Mongelli. The first model refers to the acquisition of measurements from a source by means of sensors deployed at different distances, and measuring random variables correlated with the source output. The acquired values are transmitted to a sink, where an estimation of the source has to be constructed, according to a given distortion criterion. The second model represents a "rich" communication infrastructure, where all sensor readings potentially bring fresh information to the sink. In the paper, the authors investigate coding strategies that obey a global power constraint and are decentralized.

As already addressed, three more papers, are focused on very novel and exciting scenarios in which Internet of Things instances based on sensor networks are going to play a starring role.

In the first, "*An IEEE 802.15.4 Wireless Sensor Network for Energy Efficient Buildings*", Chiara Buratti, Alberto Ferri, and Roberto Verdone find in the realization of energy-efficient buildings a very innovative and challenging field of application for wireless sensor networks (WSNs). What they aim at is minimizing the building energy consumption and optimizing the energy use. The eDIANA project, funded by FP7 of the European Commission through the ARTEMISIA framework, is focused on this target. Different network topologies are studied and compared and preliminary outputs of simulation studies are illustrated.

In the second, "*A Real Implementation and Deployment for Wine Production Management Based on Wireless Sensor Network technology*", Luca Bencini, Giovanni Collodi, Davide Di Palma, Antonio Manes, and Gianfranco Manes

describes a successful application of the Internet of Things concept in a challenging environmental monitoring context, concerning the remote management of a vineyard. The shown Wireless Sensor Network System is entirely set into the IoT vision, since it is a valid solution to monitor common parameters using simple, unobtrusive, commercial and cheap sensors, forwarding their measurements by the means of an heterogeneous infrastructure, consisting of wireless sensor network technology, GPRS communications, and ordinary Internet data transfer (TCP-IP protocol).

Last, in the paper "*Performance Evaluation of an IEEE802.15.4 Standard Based Wireless Sensor Network in Mars Exploration Scenario*", Renato Pucci, Demis Boschetti, Enrico Del Re, and Luca Simone Ronga, consider the opportunity to use an IEEE 802.15.4 standard based network in Martian planetary exploration context. By considering a network formed by a mobile rover and 40 sensors, they demonstrate through simulation that an IEEE802.15.4 based WSN can be used in planetary exploration context. Such WSN works pretty well, also in case of transmission within terrains with high density of rocks. The results shown in this paper, demonstrate that WSN should be used in future mission of planetary exploration, following a test campaign finalized to validate simulated and predicted data.

As a last contribution to the issue of "smart objects" (whose category RFID, Sensors, and Actuators belong to) handling, access, and interconnection within a unique IoT platform, in the present publication some reports from the most relevant projects funded by the European Commission dealing with embedded systems and enabling technologies are included. More specifically, the reader will find the papers: "*The PECES Project: Ubiquitous Transport Information Systems*", by Antonio Marqués, Manuel Serrano, "*Probabilistic Information Dissemination for MANETs: the IPAC Approach*", by Odysseas Sekkas, Damien Piguet, Christos Anagnostopoulos, Dimitrios Kotsakos, George Alyfantis, Corinne Kassapoglou-Faist, and Stathes, and "*HYDRA: A development platform for integrating wireless devices and sensors into Ambient Intelligence systems*", by Markus Eisenhauer, Peter Rosengren, and Pablo Antolin.

5   Security and Privacy Issues

Security and privacy issues are a central problem in all ICT scenarios. As such, security has received a lot of attention in the past and is today part of the fundamental know how of any engineer working in all ICT fields. In recent years, attention on the privacy issues raising in several communication scenarios is increasing. Indeed, privacy is recognized among the fundamental human rights and, as the pervasiveness of communication technology increases, new efforts are focusing on privacy problem from both a legislative and technical point of view.

In the IoT case, security and privacy become even more critical as their support becomes more difficult. The reasons of such difficulties lay in both the amount and sensitivity of data that will be generated and will flow through the network, and the

limitations of the computing and communication devices which will be included in the IoT and that are, therefore, much more vulnerable to all kind of security and privacy attacks.

In fact, note that in the IoT concept, objects communicate between themselves and with the information and communication infrastructure as they interact with human beings in everyday life. Therefore, it is evident that in this process they will handle information that could be fused to gain sensible insights into the habits and actions of humans. Furthermore, observe that personal information might be required to deploy added-value context-aware services. In this case, it is important to guarantee that such information is utilized only for the purposes of the service and the only information strictly needed is disclosed to the service provider. Control on the possession and the flow of such information is a must to guarantee an acceptable level of privacy. To this purpose, we observe that the lack of support of a sufficient level of privacy may jeopardize the acceptance of the IoT technologies from a societal point of view.

As we already said, WSNs and RIFD will play an important role in the IoT. Such technologies are characterized by extremely strict resource limitations. In fact, their processing capabilities will be much lower than other computing and communication technologies. Furthermore, their batteries will have low capacity and will be difficult to be replaced or, in case of RFID, they may not have autonomous energy supply at all. Such limitations must be taken into account as a constraint in the design of solutions supporting privacy and security. This basically requires that the proposed solutions must be simple and robust to system failures.

In the paper entitled "*An Overview of Privacy and Security Issues in the Internet of Things*", by Carlo Maria Medaglia and Alexandru Serbanati, the authors provide a survey on the above problems. Both wireless sensor networks and RFID technologies are considered and analysis encompasses both the short term and the long term technologies. Where the short term regards technologies that are already available or will be ready soon; whereas the long term regards technologies that today can only be envisioned. In the context of wireless sensor networks, the problems taken into account are authorization of nodes to join the network so that denial of service attacks are prevented, authentication, and data confidentiality and integrity. In the RFID case, the above problems are also taken into account considering that RFID tags always respond to readers (the user cannot decide when and to whom RFIDs should respond). The analysis suggests that all possible solutions should be set in the standardization effort, which will be the key enabling factor of the IoT technology as a whole.

A more detailed analysis of the privacy issues when RF tags are taken into account is presented in the paper "*Privacy Challenges in RFID Systems*" by Yong Ki Lee, Lejla Batina, and Ingrid Verbauwhede. In fact, RFID systems require a specific study as the solutions that have been recently proposed to guarantee privacy in systems with scarce resources cannot be applied effectively in RFID systems. In fact such solutions do not have the scalability properties, the robustness to cloning, replay, tracking, and DoS attacks, that are required in RFID systems. Accordingly, in the above paper, an analysis of the privacy threats is provided along with the

solutions proposed up to date. Solutions of such threats lay in the design of efficient and effective schemes for data protection (which involve secure algorithms for the exchange of the keys) and authentication. In such an analysis, besides standard solutions, the schemes recently proposed by the research community have been considered as well.

A possible set of solutions to the privacy problems in RFID systems is provided in the paper "*Security and Privacy Protection in Contactless Devices*" by Olivier Savry and François Vacherand. The solution proposed in this paper aims at two different objectives. The first one is to build a mechanism to offer to the user the capabilities to control the information that is released by the RFIDs. More specifically, such a scheme should allow the user to decide and control who can read any of her/his RFID tags as well as when and where this task can be accomplished. Such a management information is handled by a specific device called "Contactless privacy manager". Such device jams the transmissions of an RFID tag when it should not be read. The second objective of the proposed solution is to protect the information transmitted by an RFID. This is achieved by modulating the signal emitted by the RFID with a pseudo-noise. In this way, the RFID can be read and intercepted only by readers that can generate the same pseudo-noise. Accordingly, the seed utilized to generate the above noise can be used as a cryptographic key. The proposed solution has been implemented.

Finally, the paper "*Private Location-Based Information Retrieval via k-Anonymous Clustering*" by David Rebollo-Monedero, Jordi Forné, and Miguel Soriano deals with the problem of location privacy when user localization is a parameter utilized for the provision of context aware service. Indeed, most of the context aware services that will be deployed in the IoT need knowledge of the position of the user. However, the precision of such an information may change depending on the specific application. Accordingly, appropriate solutions should be found able to tradeoff the precision required by the application with the location privacy desired by the user. In this paper, authors propose to use the k-anonymity concept. An appropriate network element called "trusted third party" (TTP) receives location information of all the users. Then, location privacy is achieved by letting the TTP disclose location information with a precision such that the position of more than k users cannot be distinguished from each others. In this way, for example, higher level of privacy can be guaranteed in densely populated areas. The proposed solution uses a modification of the Lloyd algorithm to introduce the right amount of distortion in the location information, while the Levenberg-Marquardt algorithm is applied to adjust the quantization cell size in order to satisfy the privacy constraint.

Cagliari, Italy   Luigi Atzori
                                                                                       Daniele Giusto
                                                                                       Antonio Iera
                                                                                       Giacomo Morabito

Contents