M2M-Based Metropolitan Platform for IMS-Enabled Road Traffic Management in IoT

Luca Foschini, DEIS – University of Bologna
Tarik Taleb, NEC Laboratories
Antonio Corradi, DEIS – University of Bologna
Dario Bottazzi, Laboratori Guglielmo Marconi

ABSTRACT

Machine-to-machine communications are gaining tremendous interest from mobile network operators, equipment vendors, device manufacturers, as well as research and standardization bodies. Indeed, M2M is a promising technology for the development of Internet of Things communications platforms, with high potential to enable a wide range of applications in different domains. However, providing suitable answers to the issues stemming from IoT platform design requires middleware-level solutions to enable seamless interoperability between M2M-based applications and existing Internet-based services. To the best of our knowledge, available proposals in the field are still immature and tend to be proof of concept prototypes that address specific issues stemming from IoT domains. This article starts from a different perspective and aims at investigating the possibility of implementing M2M solutions on top of currently available, mature, production-level solutions. In this vein, we here present and discuss the design and implementation of an M2M application in the field of road traffic management that integrates, for the sake of efficiency, with a broad IMS-based service infrastructure.

INTRODUCTION

During the last decade, several research efforts have investigated emergent Internet of Things (IoT) application scenarios, where heterogeneous devices, spanning from smartphones and wireless sensors up to network-enabled physical objects (e.g., radio frequency identification — RFID, smart visual tags), can seamlessly interoperate in globally integrated communications platforms [1]. Along the same line, with the main goal of enabling direct communications with electronic devices via existing mobile operator network infrastructures (e.g., Third Generation Partnership Project's Evolved Packet System — 3GPP's EPS) in the IoT, machine-to-machine (M2M) technology has recently emerged as a promising enabler for the development of new solutions in a plethora of IoT application domains, including transportation, healthcare, ambient assisted living, smart energy, smart utility metering, supply and provisioning, city automation, intelligent tracking, manufacturing, and so forth [2].

Because of the growing demand for M2M-based services, various standardization bodies, such as 3GPP, the Open Mobile Alliance (OMA), IEEE, and European Telecommunications Standards Institute (ETSI), have recently promoted various standardization activities on M2M [3]. In brief, M2M enables highly scalable direct communications among wireless enabled heterogeneous terminals, called M2M devices, and between M2M devices and central application servers, called M2M servers [4]. The ultimate goal of these standardization activities is to leverage widespread integration of M2M devices with any existing service-level solution. However, addressing integration in IoT application domains is a very challenging issue, and, to the best of our knowledge, despite the great interest and relevant research efforts, no commonly agreed solution has been identified so far. Nevertheless, it seems natural to follow middleware-level approaches to address M2M integration issues, and to simplify the development and support of emergent M2M applications [5].

Several research efforts to address the above issue are still underway. However, available solutions are still proof of concept prototypes and cannot easily be adopted in production environments. These considerations therefore raise several challenging research questions. How can we integrate emerging M2M solutions in available platforms? Can we rely on standards and widespread solutions to leverage M2M services and applications? Can we use mature production-level software components to actually implement M2M applications?

0163-6804/11/$25.00 © 2011 IEEE

The article addresses the above issues and builds on practical experiences we had in the design of an M2M application for metropolitan traffic management that serves the needs of the Municipality of Bologna, Italy. In particular, we here discuss the adoption of the IP Multimedia System (IMS) to M2M realms. For the sake of description simplicity, we focus on the description of development and integration of a retractable bollard management solution[1] that permits restricting vehicular access to protected areas.

In our solution, the adoption of IMS was driven by various considerations. First of all, the Municipality plans the adoption of IMS to support different services, such as video surveillance, traffic condition management, automatic detection and sanction of cars that do not stop when the traffic light is red, and so forth. As a consequence, IMS seemed a natural solution to simplify the integration of M2M applications in a wider municipal service ecosystem. In addition, on one hand, IMS is an excellent integration framework that permits to take full advantage of legacy solutions, thus preserving past investments; and on the other hand, IMS makes it possible to effectively interact with internal M2M mechanisms and coordinate M2M device communications to encompass relevant aspects of communication management, such as congestion and overload control [2]. Finally, in our deployment scenario the adoption of IMS makes it possible to simplify the service management process, as involved technical staff requires only limited training to administer and maintain a new IMS-based system.

The article is organized as follows. We discuss the state of the art in the field and provide background information on M2M, IMS, and integration management in IoT deployment settings. We present the retractable bollard management case study, wherein we provide relevant insights on system architecture and implementation. Concluding remarks follow.

Background and State of the Art

This section first briefly introduces some needed background material about M2M and IMS. It then reports about some approaches that aim to cover the challenging and still open integration issues in IoT field.

Background on M2M and IMS

Currently, there are several different ongoing M2M-related standardization activities. This section describes mainly the standardization activities of 3GPP. Let us introduce a few core nodes of the 3GPP EPS network that realize basic functions used by both M2M (mainly) and IMS [4]. Evolved Node B is the mobile network base station (eNB, or base station, BS, in 3G). The home subscriber server (HSS) is the database storing authentication data and profiles for clients, ranging from M2M devices to IMS-enabled clients. The serving gateway (S-GW, or serving general packet radio service, GPRS, support node — SGSN —in 3G) acts as a local mobility anchor node. Finally, the packet data network gateway (PDN-GW, or gateway GPRS support node, GGSN, in 3G) interfaces the mobile operator network with the different packet data networks (e.g., the Internet).

M2M standards define a reference architecture and communication protocols to enable interactions between M2M devices and M2M servers [3, 4]. Typically, M2M devices either transmit or receive a predefined amount of data at a specific frequency; for instance, a pollution meter sending measurement results every day at 8:00 a.m. Within the framework of 3GPP, available standardization proposals suggest that each M2M device should contain a SIM card to authenticate with a mobile network [4]. An M2M device (called machine type communication [MTC] device in 3GPP terminology) can support different M2M features (e.g., time controlled transmission, low mobility, and infrequent transmission) to optimize the network usage by M2M applications: these features are enabled by M2M subscriptions stored in the HSS. In order to limit communications and avoid (possible) congestion situations over the cellular mobile network, a core M2M standard design guideline is that M2M devices should operate offline most of the time and connect to the mobile network only when needed.

IMS sits atop EPS core nodes to realize application-level session control through the following main functional entities [4, 6]. The IMS client is the session control endpoint, and participates in session setup and management via Session Initiation Protocol (SIP) extensions specified by the Internet Engineering Task Force (IETF) and 3GPP IMS-related standards; HSS stores HTTP-like URIs (e.g., sip:user@domain) to identify any IMS client. The application server (AS) allows the introduction of new IMS-based services. For instance, IMS enables M2M servers to be realized as specific ASs, and M2M devices hosting an IMS client can be controlled by and participate in IMS dialogs. Proxy-/interrogating-/serving-call session control functions (P-/I-/S-CSCF) are the core entities of IMS. They realize several main functions, including localization, routing out/ingoing SIP messages, associating an IMS client with its S-CSCF (as indicated within the client profile), and modifying the routing of specific types of SIP messages to ASs depending on filters/triggers specified by client profiles (IMS filter criteria) maintained by the HSS. 3GPP has also standardized some common IMS services such as the Presence Service (PS) that, following a publish/subscribe model, allows users and hardware/software components to publish data to interested entities previously subscribed to the IMS PS server, defined as presentities and watchers, respectively. Further details about M2M and IMS are available at [3, 4, 6].

Related Work on Integration Management Issues in the IoT

The IoT research field works over the growing maturity of several related technologies, such as wireless sensor networks, RFID devices, M2M, and so forth. The growing interest in this area is also demonstrated by the recent special issue of *IEEE Wireless Communications* on IoT [1].

In order to limit communications and avoid (possible) congestion situations over the cellular mobile network, a core M2M standard design guideline is that M2M devices should operate offline most of the time and connect to the mobile network only when needed.

[1] *Bologna metropolitan transportation web site, retractable bollard system web page: http://www.comune.bologna.it/trasporti/servizi/2:3023/4263/Consortium: http://www.pc104.org/*

The design of a retractable bollard management solution seems a straightforward technical activity. However, despite the apparent simplicity, various aspects complicate its development.

Despite the encouraging results obtained so far, most research works tend to mainly focus on specific technological issues (RFID tag reading speed, security, etc.). Only recently, a few research efforts have started to tackle IoT management issues rising from the full integration of M2M devices, non-computing entities, and (traffic management) services [5]. In the following, for the sake of brevity, we sketch a limited selection of solutions close to our envisioned approach, starting from those addressing lower layer aspects, at the M2M and IMS levels, and continuing with applications tackling integration issues of IoT architectures at the service level.

As evidence that M2M is becoming an important part of the communication system, some researchers have recently started to discuss M2M wireless communication overload issues [2, 7]. The work in [7] presents an analytical study aimed at modeling M2M device communication load in metropolitan areas, such as urban London, Taipei, and Beijing, and proposes possible optimizations to reduce the load at the SGSN, especially for high numbers of M2M devices in idle mode. The work in [2], instead, proposes bulk M2M signal handling to reduce the number of transmissions between eNB and the core network nodes (e.g., mobility management entity, MME). The research work on IMS as an enabler for the integration of M2M devices and wireless sensor networks (WSNs) with mobile networks is still in its infancy. The work in [8] analyzes an IoT monitoring scenario where IMS-enabled cell phones are opportunistically exploited to harvest urban monitoring data of interest from sparse WSNs deployed in the city. iRide, instead, is an IMS application that takes real-time information about traffic situations from wireless sensors installed directly on the road surface, processes them at the server side, and reports them to drivers using IMS [9].

At the service level, several successful IoT industrial and academic research initiatives are exploring traffic management solutions. For instance, there are already various applications to inform car drivers willing to park at a parking area[2] and similar projects to monitor free parking lots;[3,4] these projects are important and demonstrate the growing interest in this application domain. From a technical perspective, although addressing different application domains, we can consider two recent research efforts focusing on service integration and architectural issues of IoT with an approach close to ours [5, 10]. The first describes lessons learned during the development of web-based IoT tools and applications aimed to facilitate management and control of personal RFID tags at the University of Washington [10]. This work highlights the importance of introducing easy-to-use ad hoc web-based user interfaces to geolocalize and manage things, and to integrate IoT with existing services such as Twitter. The second, instead, calls for a radical change "from today's Intranet of things" to the "future Internet of things" and indicates as core priorities the definition of an architectural reference model for the interoperability of IoT systems and mechanisms for efficient integration of IoT architectures into the service layer of next-generation future Internet networking infrastructures [5]. However, the work focuses on the management of a WSN-equipped university building, and does not consider the possibility to exploit already available and deployed technologies (e.g., M2M and IMS) to fully integrate mobile operator infrastructures, M2M devices, and (pre-existing) services in a truly unique and valuable next-generation IoT management platform as in our proposal.

Retractable Bollard Management Case Study

The design of a retractable bollard management solution seems a straightforward technical activity: all authorized citizens are provided with credentials, and, before getting access to a restricted traffic area, are required to authenticate themselves to the system via a simple user interface; if the provided credentials are valid, the system retracts the bollard and permits vehicular access to the restricted area in the city center.

However, despite the apparent simplicity, various aspects complicate the development of a retractable bollard management solution. The system must be integrated in a broader architecture that provides advanced support to various aspects of traffic management, such as video surveillance of streets, detection and sanction of various illicit driving behaviors, and so forth. In addition, the set of citizens enabled to enter a defined protected area tend to frequently change with time, and it is subject to complex regulation that may vary according to the emerging needs of the municipality. For example, an individual could be granted the possibility to enter an area with restricted vehicular access only during work days and at a specified time (e.g., to take her children to a school downtown). Others could be granted permission to enter in a restricted area only for a short time (e.g., to reach a hotel). Finally, a further problem is system dependability. In fact, traffic concentrates in specific peak hours (e.g., morning and evening) when people leave/return to their houses, and any fault of the service at these times may seriously compromise the mobility of the city center. Hence, the system should provide easy-to-use tools to promptly detect possibly occurring problems, to let workers in the field easily locate the faulty bollard and run diagnostic processes from their mobile devices, such as iPad tablets.

M2M technologies are particularly promising for addressing the issues stemming from the retractable bollard case study. The implementation of the retractable bollard architecture would not justify the deployment of expensive broadband networking solutions. On the contrary, the widespread availability of GPRS/Univeral Mobile Telecommunications System (UMTS) technologies can offer viable and cost-effective networking opportunities. In addition, wireless networking solutions simplify large-scale outdoor system deployment, especially in road traffic management application domains (e.g., to provide suitable networking support to traffic tolls and traffic information screens). In this scenario, each retractable bollard can be equipped with an M2M device in charge of coordinating with a central M2M server to obtain the list of creden-

[2] *WorldSensing Smart Cities, automated detection of cars in parking spots: http://www.worldsensing.com/smart-cities*

[3] *University of Guelph, smart parking lot project: http://www.uoguelph.ca/~qmahmoud/fyp/nidal-nasser-3.pdf*

[4] *Meshnetics, ZigBee parking automation: http://www.meshnetics.com/ZigBee_Parking_Automation_Case_Study.pdf*

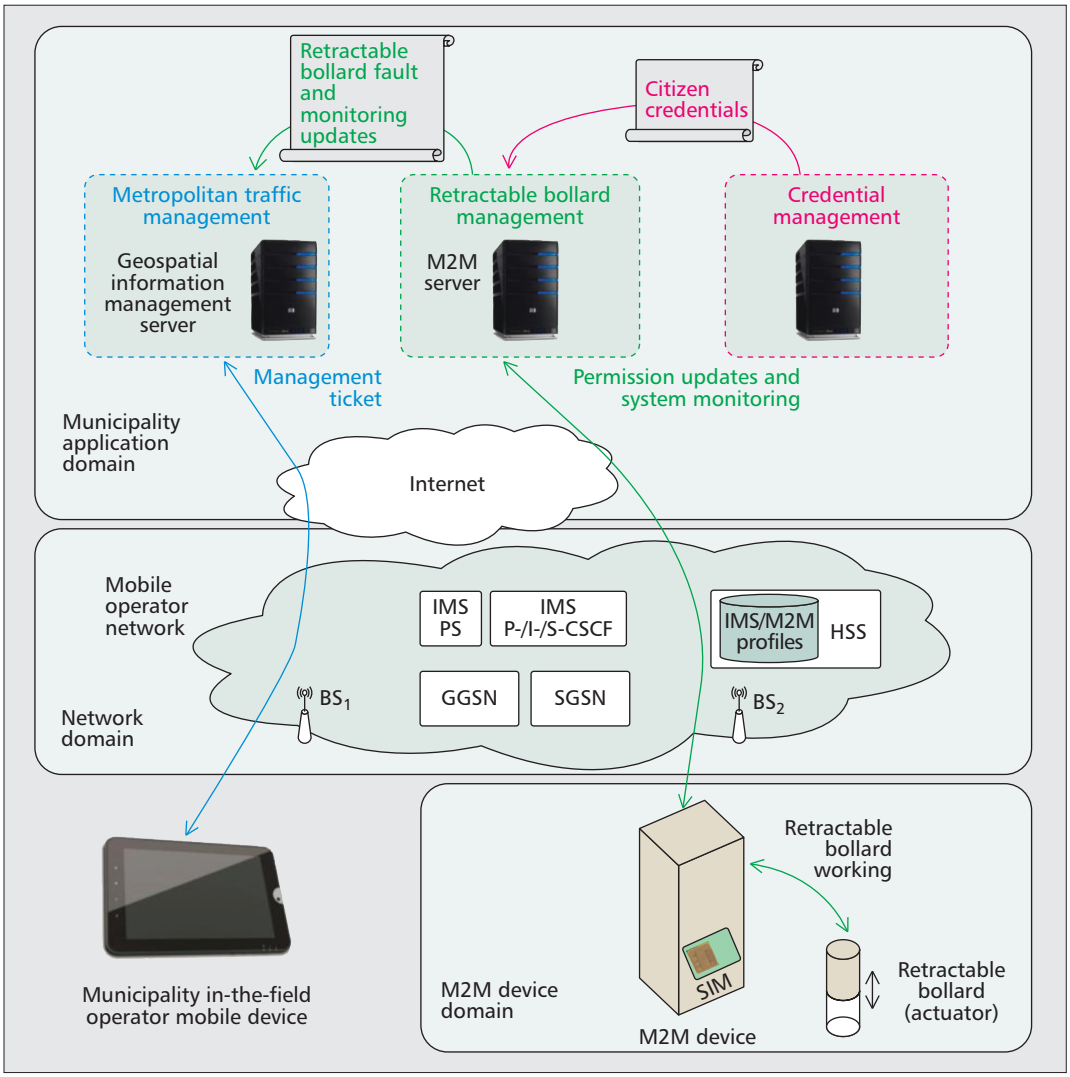

Figure 1. *IMS-enabled M2M-based retractable bollard management scenario.*

IMS is particularly well suited to realize advanced service management platforms able to integrate different infrastructures and service components according to specific application domain requirements.

tials of authorized citizens who are allowed to enter the restricted area, to obtain updates to this list, and to communicate possibly occurring failures. In addition, the M2M device can take advantage of various input channels to let citizens provide their access credentials, and of the downstanding hardware support to control the bollard and to verify its status of operability. Municipality mobile operators can locally check the bollard's functionality for prompt recovery.

The need to seamlessly integrate the system with a broader service architecture suggested the adoption of IMS as the basic communication management support. IMS provides rich, widespread, and production-level support for the development of novel services easy to integrate with existing mobile operator networks, and also with other wireless infrastructures such as Wi-Fi if available, to further cut running costs. As a consequence, IMS is particularly well suited to realize advanced service management platforms able to integrate different infrastructures and service components according to specific application domain requirements.

Following our main design guidelines, we sketch our IMS-enabled M2M-based management system in Fig. 1. It consists of three main domains. Each retractable bollard hosts an M2M device that participates to the *M2M device domain*. In the *network domain*, we show the most important 3GPP EPS nodes and IMS components that enable the communication between M2M device and M2M server via the mobile operator network.

In the *municipality application domain*, the M2M server is the service integration core component: it interacts with M2M devices via IMS, provides suitable support to authorize citizens to access restricted areas by interacting with a credential management server to obtain currently applicable citizens' credentials, and interacts with the metropolitan traffic management system. Each retractable bollard is associated with a list of citizens who have permission to access the area it protects. This information is periodically updated by the M2M server to the retractable bollard, and all valid credentials are locally stored within the M2M device to increase the reliability of the authorization process (which can complete locally at the bollard) and to limit the M2M device-to-server communication overhead. During these periodic contacts, M2M

Thanks to IMS-enabled M2M server scheduled communications, the M2M device is offline most of the time and connects to the network only when indicated by the M2M server to refresh citizen credentials and upload authenticated accesses.

device also updates authorized accesses and local management state, such as actuator fault, at the M2M server. M2M server exploits that information to update the metropolitan traffic management system, called INVENTO,[5] a web-based geospatial information management console used by municipality operators to remotely monitor continuous operability of deployed retractable bollards and issue management tickets for needed in-the-field interventions via IMS PS. Via INVENTO and our IMS-enabled platform, M2M devices become Internet-connected objects directly manageable through a highly intuitive and easy-to-use web interface.

System Architecture, Implementation, and Experimental Results

This section details all the main distributed components by focusing on interaction protocols and layered software architecture, and then presents some implementation details and seminal experimental results.

Distributed Architecture

Apart from the authentication, authorization, and accounting (AAA) server that stores citizen vehicle authorization data, our distributed architecture consists of three main components: the M2M server, the M2M device, and INVENTO.

The M2M server is the core integration component that glues together M2M devices with authentication functions and high-level management applications; it realizes two main functions. On one hand, the bollard authorization component (BAC) periodically queries the AAA server (by using SQL queries, shown as dotted lines in Fig. 2) to obtain the list of vehicles that can be admitted in each limited vehicular traffic area, and updates it to M2M devices using standard IMS PS SIP-based message exchanges managed by the IMS AS component (continuous lines); in particular, the M2M server realizes the presentities for all vehicle restricted areas, while each M2M device, acting as a watcher, subscribes only to the areas of interest (possibly more than one, e.g., when it serves a border region crossing different areas). To limit the number of M2M devices concurrently connected to the cellular M2M infrastructure, the BAC schedules M2M device publication time intervals by enclosing it within the IMS PS publish message sent to the group of devices. On the other hand, the M2M server subscribes as an IMS PS watcher to all M2M devices (also acting as presentities) to receive the list of authorized citizens that the BAC promptly updates in the AAA server, and retractable bollard failure notifications that the bollard diagnosis component (BDC) filters, aggregates, and sends to INVENTO (dash-and-dotted RESTful interactions managed by the web services, WS, communication component in Fig. 2) that visualizes those events to the final human operator.

To further reduce IMS PS traffic and avoid congestion on the last hop wired-wireless M2M communication link, we use different optimization techniques including already standardized ones, such as resource lists to enable multiple subscriptions through one only SUBSCRIBE message and partial notifications to reduce NOTIFY message length.

The M2M device interacts with the M2M server to receive citizen credential updates, and publish authorized accesses and possible failures (via the IMS client component). Thanks to IMS-enabled M2M server scheduled communications, the M2M device is offline most of the time and connects to the network only when indicated by the M2M server to refresh citizen credentials and upload authenticated accesses. Accordingly, all retractable bollard integration and management logic has been realized in such a way that it is executed locally while the M2M device is in disconnected mode; in particular, the M2M device consists of three main components. The authorization manager takes over user AAA activities: users identify themselves by means of an RFID card, and the authorization manager periodically sends an updated list of authorized vehicles to the M2M server. In order to avoid violations, authorized vehicle lists are compared against vehicle license plates (also stored by the AAA server) collected by video traffic control gates that fully cover bollard-protected areas and all main city center access/exit streets; if the received RFID does not correspond to any of these plates, an infraction will be reported to the citizen because she is likely to have passed around her RFID. Let us briefly note that this control demonstrates the full capacity of IoT management systems not only to integrate M2M devices (through IMS) with existing services, such as INVENTO, but also to exploit non-computing entities, such as vehicles traversing the control gates, as application-level inputs. Another important M2M device component is the diagnostic procedure (DP), which implements the needed support to verify the continuous operability of all available retractable bollards by checking, at regular times, whether all of its components operate in a correct way, and the results of the diagnostics procedure are then forwarded to the server-side BDC; when multiple notifications have not been received, the server-side BDC assumes that the retractable bollard is in a faulty condition. Finally, the bollard actuator control component (BACC) executes the retractable bollard's work.

The last component is a web-based user interface that depicts the status of operability to operators of the municipality control center by showing all of the interesting information, such as allocation of the faulty retractable bollard, a verbose description of detected errors, and so forth. The interface is based on INVENTO, a commercial geospatial information management framework (GIMF component in Fig. 2) developed by Laboratori Guglielmo Marconi that supports the development of Open Geospatial Consortium (OGC)-compliant services and applications, and integrates multiple communication channels to reach operators/workers. After an error notification, the control operator can issue a trouble ticket to trigger prompt system recovery by a maintenance team working in the field. The trouble ticket event is notified by

[5] *INVENTO web page: http://invento.labs.it*

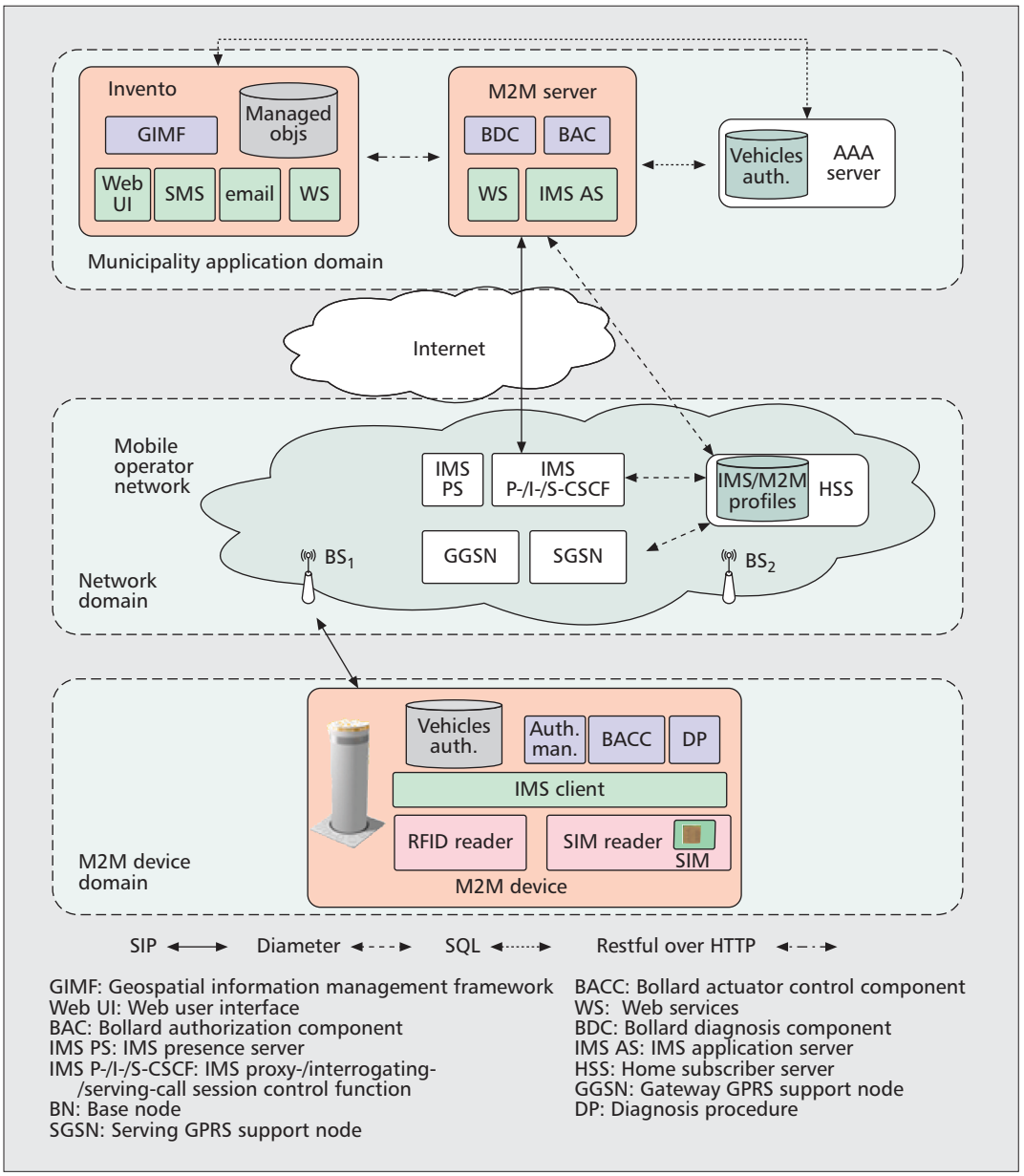

Figure 2. *M2M-based management platform distributed architecture.*

both email and IMS PS to interested maintenance team operators, and operators can rely on their mobile terminals (e.g., iPads) to access an INVENTO-based interface that permits them to easily locate faulty retractable bollards and promptly gain remote access to available diagnostic information.

System Implementation and Experimental Results

We wrap up with a brief description of the final deployed management platform implementation and deployment. Each retractable bollard comes with an M2M device developed atop a PC/104[6] Linux-based PC board equipped with an RFID reader and a SIM card (shown in Fig. 3).

The M2M server and all fixed servers, including IMS infrastructure components, instead run on powerful Linux boxes. In the near future, we are considering the possibility of moving these fixed infrastructure components, currently deployed on premises, into the cloud with several advantages in terms of both system elastic scalability and high reliability. For software components, we employed the OpenIMSCore, an IMS platform fully compliant with 3GPP IMS specifications that provides all the basic components of the IMS infrastructure (P-/I-/S-CSCFs and HSS). M2M device and server IMS modules are based on the eXosip stack, and OpenSIPS is employed for the IMS PS server. INVENTO integrates and implements widespread industrial standard protocols and technologies promoted within the framework of OGC: it includes a web map server (WMS) that permits users to be provided with proprietary raster maps and relies on the WMS standard to obtain maps from third parties (e.g., Google Maps and Bing). Finally, INVENTO enables a web-based user interface (Fig. 4) that provides active mapping features by exploiting the OpenLayers visualization support.

In the near future, we are considering the possibility to move these fixed infrastructure components, currently deployed on premise, in the Cloud with several advantages in terms of both system elastic scalability and high reliability.

[6] *PC/104 Embedded Consortium: http://www.pc104.org/*

Our work demonstrates that following the core system integration design guideline, from both technical and organizational process points of view, permits to exploit already available service and IoT technology assets to fast (re-)design novel IoT services and applications as requirements and/or municipal laws change.

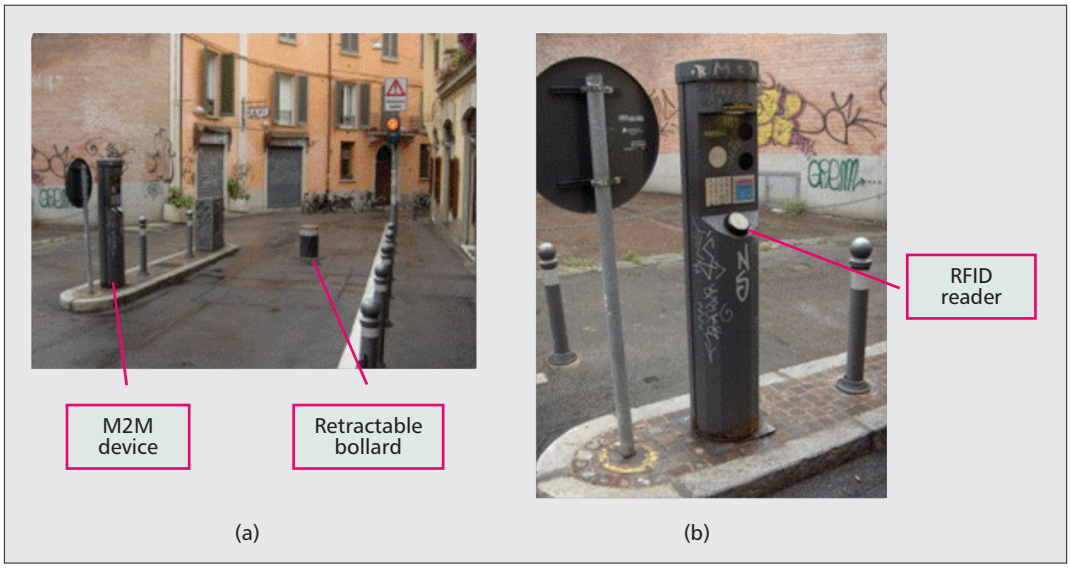

Figure 3. *a) The retractable bollard deployment, controlled by an M2M device interface; b) equipped with the RFID reader.*

We have already started collecting some seminal experimental results from our implementation. Our current testing deployment consists of 18 retractable bollards installed at core city center crossings (the final deployment will include 146 bollards). Each day, there are an average of 286 accesses for each bollard. Those accesses are typically concentrated during the peak rush hours as follows: 88 accesses between 8 a.m. and 9 a.m., when people leave their houses to go to work; 90 between 1 p.m. and 2:30 p.m., when some people get back home for lunch and then go back to work (about 50 incoming and 40 outgoing accesses), and about 108 between 6 p.m. and 7 p.m., when people return home after work.[7] In the worst case situation in the evening, our system has to process $(108 \times 18)/60 = 32.4$ authorized access updates/min, about 1 update every 2 s.

That frequency is already high for M2M. In fact, given the small dimensions of the Bologna city center, most of the M2M devices attach to the same BS node; in addition, we are using M2M communications where, for example, the default value for the average time period between M2M device location updates is 56 min [2]. Thanks to our IMS-enabled communications controlled by the M2M server, we are able to evenly schedule M2M device transmissions to have a maximum of about 4 updates/min. Let us note that we could have also used the time controlled transmission feature available at the lower M2M level, but it would have required continuously updating M2M device subscriptions at the HSS, while our IMS-operated communication scheduling is much more flexible and can promptly adapt to load changes. The cost is as low as publishing an IMS PS message of about 500 bytes to coordinate M2M devices.

To conclude, this article stresses the central role of highly integrated organizational processes in applied research in the IoT field, especially in metropolitan traffic management. In fact, our work demonstrates that following the core system integration design guideline, from both the technical and organizational process viewpoints, permits already available service and IoT technology assets to be exploited to quickly (re)design novel IoT services and applications as requirements and/or municipal laws change.

Conclusions

In the years to come, IoT-based services and applications are likely to become an integral part of our everyday life. Basic technologies that leverage seamless interaction between unconventional artifacts (i.e., real life resources) have already been developed and play a relevant role in different application domains, such as logistics and road traffic management.

The present work describes the design of an integrated IoT retractable bollard management system to rule vehicular access to restricted city areas based on standard infrastructures and software components. The article also discusses the main design guidelines to consider in system development. In particular, the article stresses the necessity of integrating IoT-based services within the framework of enterprise management solutions, relying on standard solutions, and providing suitable support to simplify system maintenance and management.

Acknowledgments

We sincerely thank the Municipality of Bologna for the kind collaboration on this research. This work was partially supported by the EU Project CIVITAS MIMOSA.

References

[1] A. Iera *et al.*, Ed., Special Issue on the Internet of Things, *IEEE Wireless Commun*, vol. 17, no. 6, 2010, pp. 8–9.
[2] T. Taleb and A. Kunz, "Machine Type Communications in 3GPP Networks: Potential, Challenges, and Solutions," to appear, *IEEE Commun. Mag.*
[3] 3GPP, "System Improvements for Machine-Type Communications," TR 23.888 V1.3.0, June 2011.

[7] *The number of accesses incoming and outgoing is different due to the high number of one-way streets in the city center and different restriction applied to the different traffic directions, namely incoming accesses are typically more effectively monitored.*

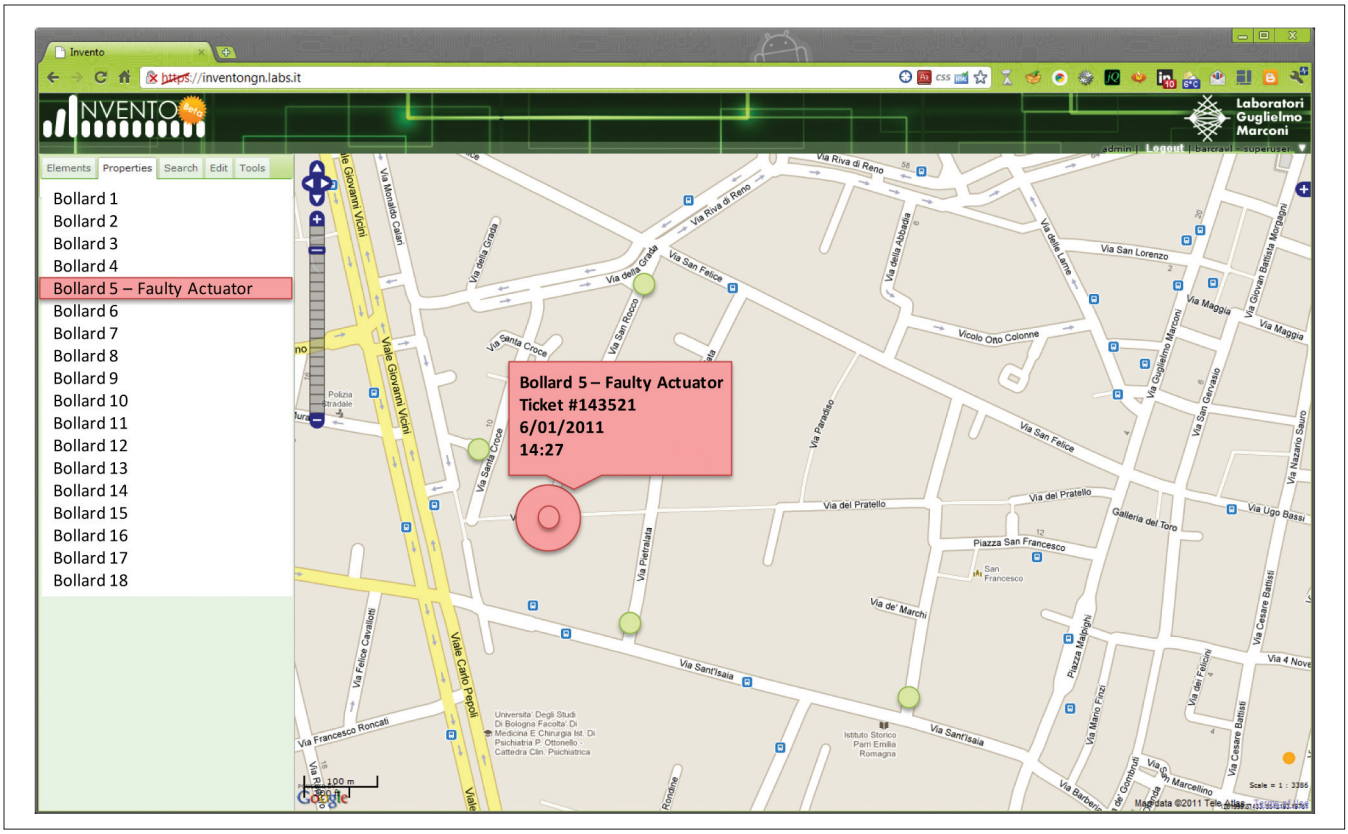

Figure 4. *INVENTO web-based user interface.*

[4] 3GPP, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access," TS 23.401, v. 10.4.0, June 2011.

[5] M. Zorzi *et al.*, "From Today's INTRAnet of Things to A Future INTERnet of Things: A Wireless- and Mobility-Related View," *IEEE Wireless Commun*, vol. 17, no. 6, 2010, pp. 44–51.

[6] 3GPP, "IP Multimedia Subsystem (IMS); Stage 2," TR 23.228 v. 11.1.0, Jun. 2011.

[7] S.-T. Sheu, Y.-T. Lee, and S. Lu, "Load Analysis for MTC Devices in Idle Mode or Detached State," *Proc. IEEE Int'l. Computer Symp. '10)*, 2010, pp. 424–28.

[8] P. Bellavista *et al.*, "The Future Internet Convergence of IMS and Ubiquitous Smart Environments: an IMS-Based Solution for Energy Efficiency," *Elsevier J. Network and Comp. Apps.*, Special Issue on Intelligent Algorithms for Data-Centric Sensor Networks, May 2011.

[9] M. Elkotob and E. Osipov, "iRide: A Cooperative Sensor and IP Multimedia Subsystem Based Architecture and Application for ITS Road Safety," *Proc. EuropeComm '09*, Springer LNCS, vol. 16, part 3, 2009, pp. 153-62.

[10] E. Welbourne *et al.*, "Building the Internet of Things Using RFID: The RFID Ecosystem Experience," *IEEE Internet Computing*, vol. 13, no. 3, May/June 2009, pp. 48–55.

Biographies

Luca Foschini [M] (luca.foschini@unibo.it) graduated from the University of Bologna, Italy, where he received a Ph.D. degree in computer engineering in 2007. He is now a research fellow of computer engineering at the University of Bologna. His interests include distributed systems and solutions for pervasive computing environments, system and service management, context-aware session control and adaptive mobile multimedia, and mobile-agent-based middleware solutions. He is a member of the Italian Association for Computing (AICA).

Tarik Taleb [SM] (tarik.taleb@neclab.eu) received his B.E degree in information engineering with distinction, and M.Sc. and Ph.D. degrees in information sciences from GSIS, Tohoku University, Japan, in 2001, 2003, and 2005, respectively. He is currently working as a senior researcher and 3GPP standards expert at NEC Europe Ltd. Prior to his current position, he worked as an assistant professor at the Graduate School of Information Sciences, Tohoku University, Japan. His research interests lie in the field of architectural enhancements to 3GPP networks, mobile multimedia streaming, wireless networking, intervehicular communications, satellite and space communications, congestion control protocols, handoff and mobility management, and network security. He is/was on the editorial boards of *IEEE Wireless Communications*, *IEEE Transactions on Vehicular Technology*, *IEEE Communications Surveys & Tutorials*, and a number of Wiley journals. He is the recipient of many awards, including the 2009 IEEE ComSoc Asia-Pacific Young Researcher award, the 2008 TELECOM System Technology Award, and the 2007 Funai Foundation Science Promotion Award.

Antonio Corradi [M] (antonio.corradi@unibo.it) graduated from the University of Bologna and received an M.S. in electrical engineering from Cornell University, Ithaca, New York. He is a full professor of computer engineering at the University of Bologna. His research interests include distributed and parallel systems and solutions, middleware for pervasive and heterogeneous computing, infrastructure support for context-aware multimodal services, network management, and mobile agent platforms. He is a member of the ACM and AICA.

Dario Bottazzi [M] (dario.bottazzi@labs.it) graduated from the University of Bologna, Italy, where he received a Ph.D. degree in computer engineering in 2004. He is now chief researcher at Laboratori Guglielmo Marconi SpA. His research interests include middleware for pervasive and heterogeneous computing, network and service management, and advanced platforms for context management.