Chapter 17:
M2M-Based Metropolitan Platform for IMS-Enabled Road Traffic Management in IoT

Chih-Yuan Lee
Department of CSIE
National Taipei University

Outline

- Abstract
- Introduction
- Background
- System Architecture
- Conclusion

Abstract

- M2M communication : (communication between) Machine-to-Machine
- A promising technology for the development of Internet of Thing (IoT) communications platforms
- 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.
- 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

- With the main goal of enabling direct communications with electronic devices via existing mobile operator network infrastructures in the IoT such as 3GPP, M2M technology has recently emerged as a promising enabler for the development of new solutions in a plethora of IoT application domains
- Various standardization bodies: 3GPP, OMA, IEEE, ETSI, …etc.
- M2M enables highly scalable direct communications among wireless enabled heterogeneous terminals, called M2M devices
- Servers between M2M devices and central application servers, called M2M servers
- The ultimate goal of these standardization activities is to leverage widespread integration of M2M devices with any existing service-level solution.

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?

Scenario

- Scenario :
  - 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.

Background on M2M and IMS

- This section describes mainly the standardization activities of 3GPP
- 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
- 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).

Background on M2M and IMS (Cont.)

- M2M standards define a reference architecture and communication protocols to enable interactions between M2M devices and M2M servers. Typically, M2M devices either transmit or receive a predefined amount of data at a specific frequency
- Within the framework of 3GPP, available standardization proposals suggest that each M2M device should contain a SIM card to authenticate with a mobile network
- 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

Main functional entities for realizing application-level session control in IMS

- 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.

- 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.
- 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

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.
- ✓ IoT management issues rising from the full integration of M2M devices, non-computing entities, and (traffic management) services

- M2M wireless communication overload issues [2,7]
- Web- based IoT tools and applications aimed to facilitate management and control of personal RFID tags at the University of Washington [10]
- “From today’s Intranet of things” to the “future Internet of things”[5]

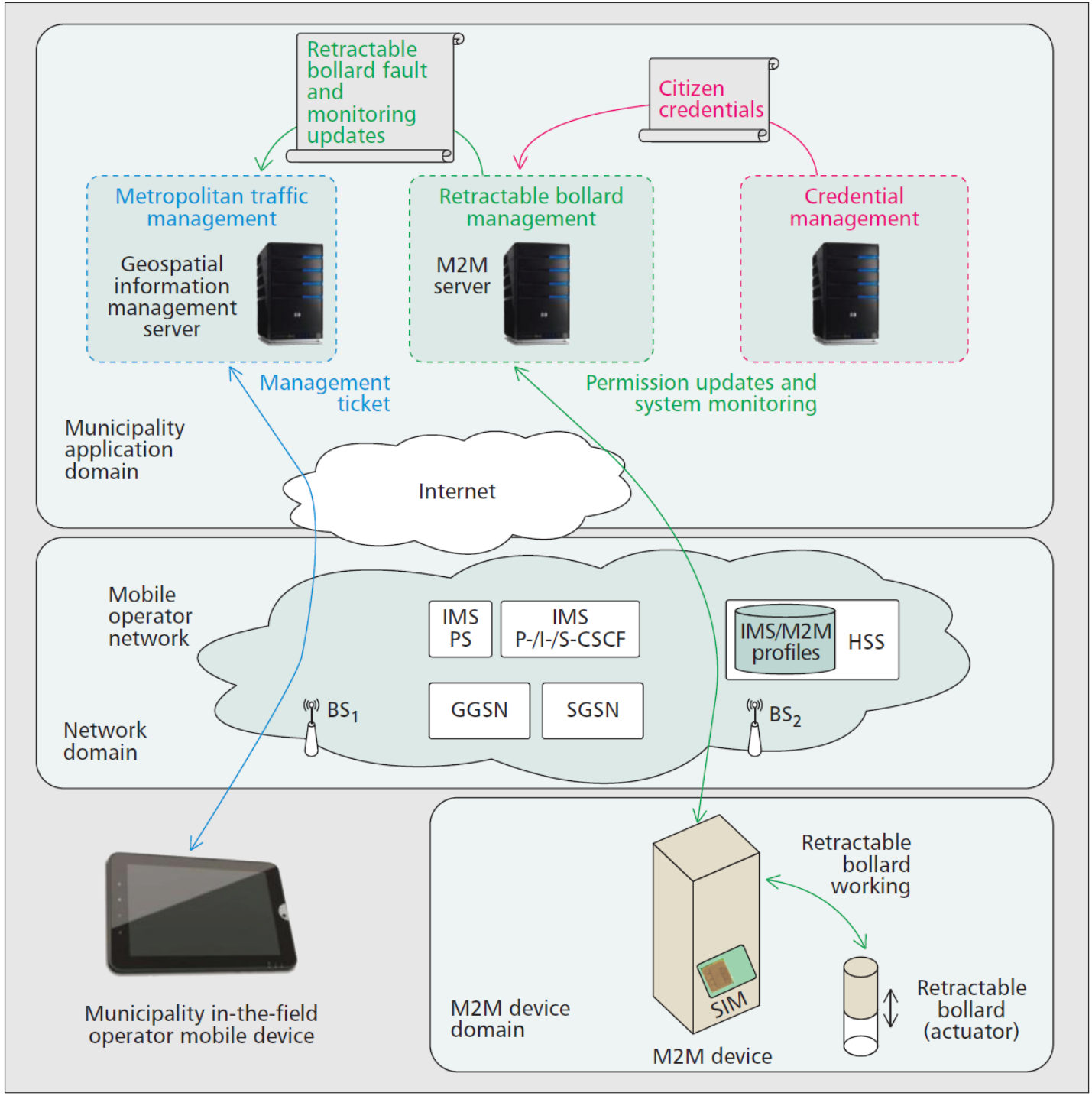
Retractable Bollard Management Case Study

- 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, the system must be integrated in a broader architecture that provides advanced support to various aspects of traffic management
- In addition, the set of citizens enabled to enter a defined protected area tend to frequently change with time
- Finally, a further problem is system dependability in peak hours

(a)

Using M2M Technologies

- M2M technologies are particularly promising for addressing the issues stemming from the retractable bollard case study
- The widespread availability of GPRS/Universal Mobile Telecommunications System (UMTS) technologies can offer viable and cost-effective networking opportunities
- Wireless networking solutions simplify large-scale outdoor system deployment, especially in road traffic management application domains
- 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 credentials of authorized citizens who are allowed to enter the restricted area, to obtain updates to this list, and to communicate possibly occurring failures.

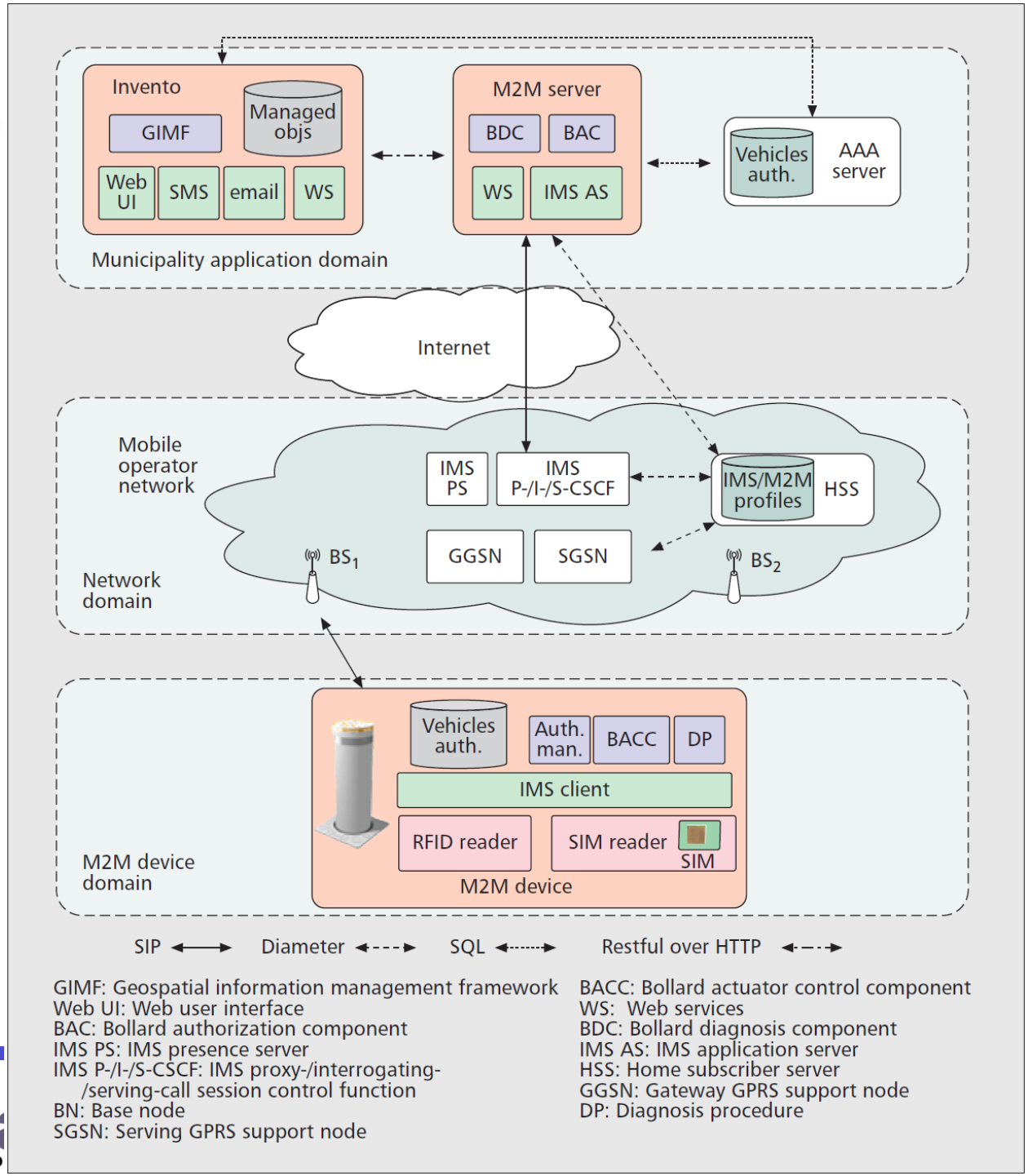

Retractable bollard fault and monitoring updates
Citizen credentials
Metropolitan traffic management
Geospatial information management server
Retractable bollard management
M2M server
Credential management
Management ticket
Permission updates and system monitoring
Municipality application domain
Internet
Mobile operator network
IMS PS
IMS P-/I-/S-CSCF
IMS/M2M profiles
HSS
GGSN
SGSN
BS1
BS2
Network domain
Municipality in-the-field operator mobile device
M2M device domain
SIM
M2M device
Retractable bollard working
Retractable bollard (actuator)

Three Domains in Retractable Bollard Management Scenario

- Each retractable bollard hosts an M2M device that participates to the *M2M device domain*
- In the *network domain*, here shows 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

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(a web-based geospatial information management console)



GIMF: Geospatial information management framework
Web UI: Web user interface
BAC: Bollard authorization component
IMS PS: IMS presence server
IMS P-/I-/S-CSCF: IMS proxy-/interrogating-/serving-call session control function
BN: Base node
SGSN: Serving GPRS support node
BACC: Bollard actuator control component
WS: Web services
BDC: Bollard diagnosis component
IMS AS: IMS application server
HSS: Home subscriber server
GGSN: Gateway GPRS support node
DP: Diagnosis procedure

Distributed architecture(Cont.)

- The M2M server is the core integration component that glues together M2M devices with authentication functions and high-level management applications
  - The bollard authorization component (BAC) periodically queries the AAA server to obtain the list of vehicles that can be admitted in each limited vehicular traffic area, and updates it to M2M devices. 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.
  - The M2M server subscribes as an IMS PS watcher to all M2M devices 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 that visualizes those events to the final human operator.

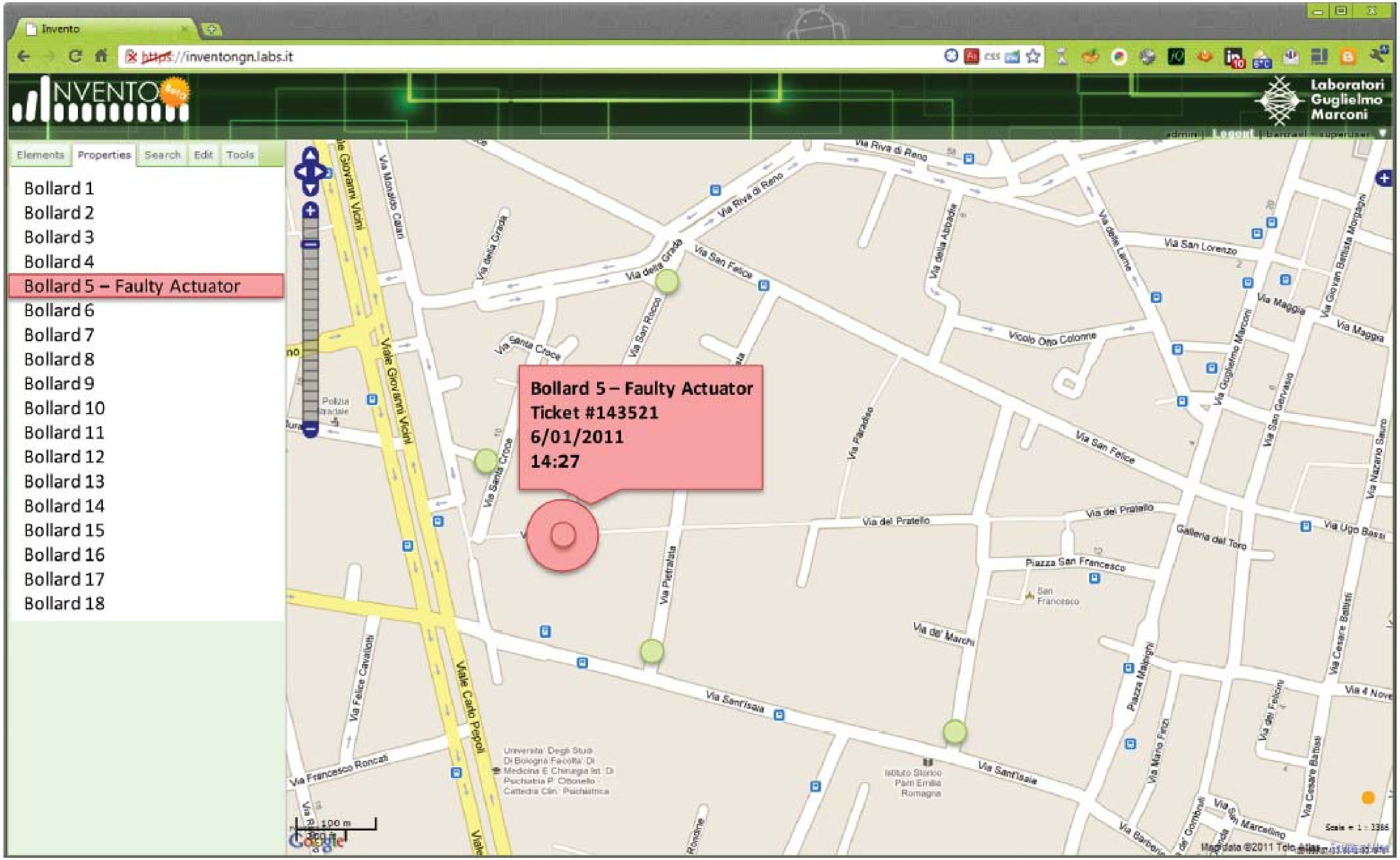
Distributed architecture(Cont.)

- The M2M device interacts with the M2M server to receive citizen credential updates, and publish authorized accesses and possible failures
- 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.
- 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 collected by video traffic control gates that fully cover bollard-protected areas and all main city center access/exit streets

(b)

Distributed architecture(Cont.)

- 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
- Bollard actuator control component (BACC) executes the retractable bollard's work.
- 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.


Invento
https://inventongn.labs.it
INVENTO
Laboratori Guglielmo Marconi
Elements
Properties
Search
Edit
Tools
Bollard 1
Bollard 2
Bollard 3
Bollard 4
Bollard 5 – Faulty Actuator
Bollard 6
Bollard 7
Bollard 8
Bollard 9
Bollard 10
Bollard 11
Bollard 12
Bollard 13
Bollard 14
Bollard 15
Bollard 16
Bollard 17
Bollard 18
Bollard 5 – Faulty Actuator
Ticket #143521
6/01/2011
14:27
Via del Pratello
Via San Felice
Via Sant'Isaia
Viale Giovanni Vicini
Viale Carlo Pepoli
Via Riva di Reno
Piazza San Francesco
Via Ugo Bassi
100 m

Conclusion

- In the years to come, IoT-based services and applications are likely to become an integral part of our everyday life
- 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.
- 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.

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.

[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.

Questions

1) What is the core M2M standard design guideline in order to limit communications and avoid (possible) congestion situations over the cellular mobile network.
2) What are the three domains of a M2M system and their functionalities.