Demo: A Rule-based IoT Intelligent Building Management System

P. Charalampidis
A. Makrogiannakis
Institute of Computer Science
Foundation for Research and Technology-Hellas, Greece
pcharala@ics.forth.gr
makrog@ics.forth.gr

J. Economou
A. Griva
Converge SA
Greece

A. Kioussis
A. Koukis
Converge SA
Greece

G. Lambropoulos
Converge SA
Greece
glabropoulos@converge.gr

I. Avgouleas
V. Angelakis
Department of Science and Technology, Linköping University,Sweden
ioannis.avgouleas@liu.se
vangelis.angelakis@liu.se

S. Papadakis
A. Fragkiadakis
Institute of Computer Science
Foundation for Research and Technology-Hellas, Greece
stefpap@ics.forth.gr
alfrag@ics.forth.gr

Abstract

In this demonstration, we present a rule-based Intelligent Building Management System (IBMS) that uses a three-tier IoT system for gathering sensory measurements and controlling specific devices based on the collected measurements and a set of user-defined rules. Our solution uses a hybrid architecture comprising both distributed and centralized components. The IoT nodes, which use the 6LoWPAN standard, communicate through a protocol translating gateway with a middleware server. The intelligence module employs a Cased-based Reasoning (CBR) engine for deciding upon (de-)activation of devices by monitoring both the result of rules' application on measurements provided by the middleware server and user reaction to the automated decisions.

1 Introduction

The Internet of Things (IoT) presents itself as a promising set of technologies that will enable the efficient interconnection of a large number of highly heterogeneous smart objects (SOs) through the Internet. By participating in this universal virtual network, SOs are not only providers but also consumers of information, enabling, in this spirit, the provision of a variety of advanced applications in several domains (e.g. environmental monitoring, e-health, smart grid).

Rapid advancements in hardware and software have substantially benefited the IoT systems, fostering the constructions of cheap miniature sensing devices that are able to measure a large variety of physical phenomena. Additionally, embedded network systems in the form of Wireless Sensor Networks (WSNs), that employ energy-efficient network protocols (e.g. 6LoWPAN, RPL, CoAP) and operating systems specifically tailored for resource-constrained devices, have acted as the main building block of existing IoT systems.

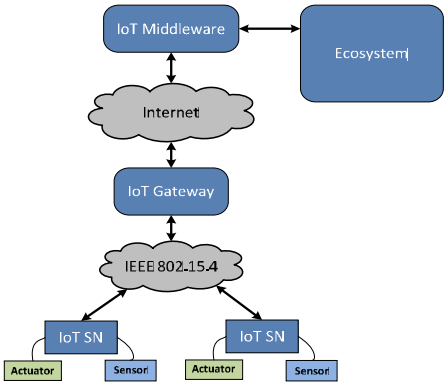

Figure 1. Proposed IBMS architecture

Among the applications promoted by the IoT paradigm, smart building management systems are of paramount importance, offering a major improvement in users' quality of life by automating everyday home activities in a personalized and context-aware manner [1, 3]. An IBMS coordinates a set of sensors and actuators that communicate with a central unit, which senses the building environment and controls the actuation of building devices, in a way transparent to the

International Conference on Embedded Wireless Systems and Networks (EWSN) 2018
14–16 February, Madrid, Spain

ISBN: 978-0-9949886-2-1

user. IoT architectures that built following security and privacy by design principles [4], can offer a reliable platform for IBMSs. A host of other IoT features, such as the flexibility for a wide variety of sensory data and the wireless connectivity together with an array of self-X properties, strengthen this claim.

In this demo, we present a rule-based IBMS that uses an IoT system to gather data from various sensors and control specific devices based on the collected sensory data and a set of user-defined rules. The architecture consists of two parts: (i) the IoT system and (ii) the Ecosystem [5] (as shown in Figure 1) that are described in the following sections.

2 The IoT system

The IoT system enabling the proposed IBMS follows conceptually a three-tier hierarchical architecture that comprises three distinct components. These are: (i) the resource-constraint IoT Sensor Nodes (SNs) that are equipped with various sensors, which produce measurements of locally observed physical phenomena, (ii) the IoT Gateway (GW) that is positioned in proximity to the SNs and autonomously processes data aggregated by them, and (iii) the IoT Middleware (MW) that plays the role of the back-end cloud responsible for virtualization, data storage and service provisioning.

SNs are built based on a Zolertia RE-Mote platform (32MHz CPU, 32KB RAM and 512MB Flash Memory) that offers dual radio operation both in ISM 2.4GHz and ISM 863-950MHz frequency band, under IEEE 802.15.4g standard. External sensors can be attached to the RE-Mote platform through a number of communication ports (e.g. I2C, SPI). IPv6 connectivity tailored for the low-power, resource-constrained nature of the RE-Mote platform is offered by the Contiki OS. Measurements collected through sensor drivers are communicated using Constrained Application Protocol (CoAP) by a CoAP server running on the RE-Mote.

SNs interact with the MW through the GW, which performs local data processing, storage and networking services [2]. It practically acts as a cross-protocol proxy that is responsible for providing network and application protocol translation. Additionally, the GW offers functionalities, such as sensor registration, monitoring and management, measurement aggregation and forwarding. Essentially, it hosts two different network interfaces. On the one side, there is an IEEE 802.15.4 interface of the 6LoWPAN border router for the sensor network, while on the other side, connectivity to the MW is provided by Ethernet or WiFi interfaces.

Finally, the MW plays the role of the system back-end, where services are invoked and data streams are managed. Its functional components are: (i) the Service Manager that handles the service requests from the applications by identifying the Virtual Entities (VEs) that are of interest for the application, (ii) the Generic Virtual Object (GVO) manager that creates and manages the digital representations of the SNs, (iii) the Federation Manager that creates and manages federations of SNs for service composition and orchestration, (iv) the Data and Context manager that adds context and performs data processing (i.e. performing averages, filtering data, etc.), and (v) the Security Manager that is responsible for the secure device configuration of the devices, secure communications, as well as the authorization and access control.

3 The Ecosystem

The Ecosystem platform belongs to the family of information systems relating to IBMS solutions, and is oriented towards both technologically experienced and non-experienced users, enabling the management of a heterogeneous group of sensors and actuators which are spread in a particular and limited space such as a room, an apartment or a house. By linking heterogeneous sensors, the Ecosystem provides information that can help the user enrich his/her existing knowledge for the environment where he/she is located, as well as provide valuable and accurate information so that the Ecosystem will take autonomously any reasonable decision. The offered automation has been designed so as to enhance the user's control on the environment by adding extra features and take reasonable decisions based on information delivered by different sensors.

The Ecosystem is implemented as a web application on Spring framework, due to its open source nature and modular architecture that allows us to focus on the implementation without unnecessary ties to specific deployment environments. The sensors and the actuators that are connected to the Ecosystem are described in XML, and Java Architecture for XML Binding (JAXB) is used to automate the mapping between these XML documents and the corresponding Java objects. The CBR module implemented is based on a rating system for the active rules. Every time a rule is activated a new monitor thread is created. This thread runs for a certain time interval and monitors whether the user changes the actuators' state, as it was automatically decided after the rule's application. If the user cancels the actions taken by the rule, the rule receives a negative rating. After a specific number of negative ratings the rule is paused.

4 Acknowledgments

This work has received funding from the European Union's Seventh Framework Program (FP7/2007-2013) under grant agreement no. 612361.

5 References

[1] B. Bach, D. Wilhelmer, and P. Palensky. Smart buildings, smart cities and governing innovation in the new millennium. In *Industrial Informatics (INDIN), 2010 8th IEEE International Conference on*, pages 8–14. IEEE, 2010.

[2] P. Charalampidis, E. Tragos, and A. Fragkiadakis. A fog-enabled iot platform for efficient management and data collection. In *2017 IEEE 22nd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pages 1–6, June 2017.

[3] O. Evangelatos, K. Samarasinghe, and J. Rolim. Evaluating design approaches for smart building systems. In *Mobile Adhoc and Sensor Systems (MASS), 2012 IEEE 9th International Conference on*, pages 1–7. IEEE, 2012.

[4] E. Tragos, A. Fragkiadakis, V. Angelakis, and H. C. Pöhls. Designing secure iot architectures for smart city applications. In *Designing, Developing, and Facilitating Smart Cities*, pages 63–87. Springer, 2017.

[5] E. Z. Tragos, M. Foti, M. Surligas, G. Lambropoulos, S. Pournaras, S. Papadakis, and V. Angelakis. An iot based intelligent building management system for ambient assisted living. In *2015 IEEE International Conference on Communication Workshop (ICCW)*, pages 246–252, June 2015.