Computers and Electrical Engineering 000 (2017) 1–10

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

An applications interoperability model for heterogeneous internet of things environments☆

R. Vinob chander[a,*], Saswati Mukherjee[b], Susan Elias[c]

[a] Department of Information Technology, SSN College of Engineering, Anna University, Chennai, Tamil Nadu, INDIA
[b] Department of Information Science and Technology, College of Engineering, Anna University, Chennai, Tamil Nadu, INDIA
[c] Department of Electronics Engineering, VIT University, Chennai Campus, Tamil Nadu, INDIA

ARTICLE INFO

Article history:
Received 12 May 2016
Revised 29 December 2016
Accepted 30 December 2016
Available online xxx

Keywords:
Smart Objects
Internet of Things
CoAP
Interoperability
REST
6LoWPAN

ABSTRACT

Objects/devices in the Internet of Things (IoT) Environments are frequently heterogeneous in nature with diverse processor (8-/16-bit) structures, operating systems, and applications in different programming languages. Consistent connection among the objects in such situations is conceivable just when the applications can speak with each other irrespective of their surroundings/implementation details. These objects are generally constrained in nature as for memory, power, throughput, cost, and form factor. In this paper, we propose an applications interoperability model for wireless embedded networks and assess it on objects that are constrained and heterogeneous in nature. Our feasibility tests demonstrate the potential benefits that can be accomplished as far as applications interoperability (especially concerning discovery, monitoring, syndication, and control) is concerned. Also, our assessment quantifies the overhead of using Simple Object Access Protocol (SOAP) and Hypertext transfer protocol (HTTP) based approaches that took roughly 1.4 to 2.7 times longer than our proposed CoAP based model.

1. Introduction

The IoT is a vital idea that uses the Internet Protocol (IP) to speak with real-world, physical objects called Smart Objects (SOs). SOs combine embedded systems, ubiquitous computing, mobile telephony, telemetry, wireless sensor networks, mobile computing, and computer networking [1]. They normally contain sensor(s) and/or actuators, a microcontroller, a communication medium, and a power source. These SOs/motes are generally constrained in nature, with just a couple of kilobytes of memory, a 8-/16-/32-bit chip, a low-power source (battery) and a wireless communication device (few hundreds of kilobits per second). They likewise cost less (a couple of dollars) and have a small (a couple square mms) form factor. SOs are broadly utilized as a part of home automation, logistics, healthcare, power grids, car parking, wildlife monitoring etc.

A noteworthy worry in realizing the vision of the IoT is applications interoperability. Basically, the SOs might be heterogeneous in nature with various operating systems (sometimes without an operating system), architectures, and languages. Application(s) in such different frameworks may need to flawlessly communicate with each other, especially when these are part of a constrained environment. To the best of our insight, existing works (see Section 2) on IoT applica-

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. S. Smys.

* Corresponding author.
E-mail addresses: vinobchanderr@ssn.edu.in, chanderr@zoho.com (R. Vinob chander), msaswati@auist.net (S. Mukherjee), susan.elias@vit.ac.in (S. Elias).

http://dx.doi.org/10.1016/j.compeleceng.2016.12.029
0045-7906/

tions interoperability use medium sized SOs with ways to deal with connectivity either as being direct or through proprietary protocols inside of a Personal Area Network(PAN) increasing the overhead of the gateway. Despite the fact that these arrangements handle IoT applications interoperability, they couldn't be applied on any heterogeneous constrained situations. Also, most research (see Section 2) has concentrated on utilizing either IPv4 or proprietary methods to network SOs. However, the need of the hour is to utilize IPv6 to interface and guarantee coordinated effort between billions of SOs, as there are no newer IPv4 addresses and much reuse of the existing addresses is not a viable option. In this paper, we propose a model for device level IoT applications interoperability using IPv6. In particular, we focus on discovery / monitoring, syndication, and control for heterogeneous constrained environments. Our contributions include testing the proposed model on heterogeneous constrained SOs and comparing the round trip time with existing SOAP and HTTP based approaches.

The rest of this paper is organized as follows. Section 2 shows a brief survey of related work and the inspiration driving this paper. Section 3 depicts our proposed REST based model and the functions of its major components. We present the evaluation method in Section 4. Section 5 has the setup and the description of the tests carried out on our proposed model. Section 6 presents the results of the tests carried out in the previous section and also compares the performance of our model with existing approaches. Section 7 concludes the paper.

2. Related work

Link layer technological advances have been changing quickly since serial connections were produced. At the point when IEEE 802.15.4 was adopted as a low power radio frequency (RF) innovation (2.4 GHz and 900 MHz), various link layers were designed (PLC, ITU, Homeplug, GreenPHY, Wavenis, Zigbee, Bluetooth Smart, low power WiFi, IEEE 802.15.4 g, and so forth.). There are two choices for interfacing with the link layer. The first builds gateways and uses tunneling and translation to transport non-IP traffic over an IP network [2]. These gateways are costly, hard to manage, and lack flexibility and scalability. The second is to utilize the IP. This is an open standard set by the Internet Engineering Task Force (IETF), which is omnipresent and has a layered design. The IP is profoundly versatile and has an extensive address space. The need to interface billions of SOs implies that using IP is the right decision for connecting with these link standards.

A noteworthy test when planning, designing, and actualizing a productive design for any IoT application is to take care of disparate environments. REST and Simple Object Access Protocol (SOAP) based web services are, by a wide margin, the two most generally utilized techniques that address applications interoperability. Authors in [3] studied the feedback from 69 developers regarding the use of WS-* based or REST based approaches for IoT. They found that developing REST based applications for accessing sensor reading was more easy and flexible than WS-* based approaches. REST is an unadulterated technique for utilizing the web design with HTTP to control resources. Authors in [4] use a REST based method for monitoring and controlling the home appliances using plogs and a smart gateway. An implementation of REST style Web services on embedded system is done by authors in [5]. [6] is a popular REST based cloud to connect and monitor SOs in near-real time. A list of major REST based IoT cloud platform providers are in [7]. HTTP is ideal for client-server applications that are pull oriented and long-lived. However, HTTP uses transport control protocol (TCP) binding and is synchronous in nature, which may not be a reasonable answer for constrained and lossy situations.

Albeit SOAP and / WS-* based solutions [8,9,10] do give a sensible workaround to interoperability for IoT applications, they are not a flawless fit for constrained environments (8-bit microprocessors, small flash and random access memory, and low bandwidth).

We thus see that existing approaches to IoT application interoperability are either direct (IP support at the device) or through a gateway making the translation. These approaches could not be used where constrained SOs within a Personal Area Network (PAN) might need to communicate seamlessly. In the following section, we propose a model where we use IPv6 on constrained nodes for device level application interoperability.

3. Proposed REST based model for constrained IoT

We propose a model called as CoAP Application Interoperability Model for IoT (CAIM4IoT) that uses IETF standards to achieve collaboration. CAIM4IoT uses IPv6 for Low Power Personal Area Networks (6LoWPAN) (RFC4944) [11], and Constrained Application Protocol (CoAP) for achieving interoperability. Fig. 1 shows CAIM4IoT for constrained smart environments, and Table 1 shows a summary of the frequently used notations/abbreviations. The following subsections provide an overview of the proposed model CAIM4IoT (Section 3.1), the model's interaction details (Section 3.2), followed by details of the IETF standards (Section 3.3) used in it.

3.1. CAIM4IoT overview

In our proposed model, a remote IoT application (SO Application in Fig. 1) can speak with SOs inside a PAN utilizing the RESTful CoAP protocol for discovery, monitoring, syndication, and control. "o/a" in Fig. 1 implies observation/actuation of the interested SO. Observation permits the SO to be monitored and activation permits the SO to be controlled (like open/close the entryway and so forth). A client request to the SO inside the PAN reaches through the border router. The border router is responsible for neighbor discovery (ND), addressing, routing using the routing protocol for lossy networks