Computer Networks 73 (2014) 98–111

Contents lists available at ScienceDirect

Computer Networks

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

The problem of task allocation in the Internet of Things and the consensus-based approach

Giuseppe Colistra, Virginia Pilloni, Luigi Atzori *

DIEE, University of Cagliari, Piazza d'Armi, 09123 Cagliari, Italy

ARTICLE INFO

Article history:
Received 3 October 2013
Received in revised form 12 May 2014
Accepted 28 July 2014
Available online 13 August 2014

Keywords:
Consensus
Resources allocation
Internet of Things

ABSTRACT

The realization of the Internet of Things (IoT) paradigm relies on the implementation of systems of cooperative intelligent objects with key interoperability capabilities. One of these interoperability features concerns the cooperation among nodes towards a collaborative deployment of applications taking into account the available resources, such as electrical energy, memory, processing, and object capability to perform a given task, which are often limited.

In this paper, firstly, we define the issue related to resource allocation for the deployment of distributed applications in the IoT, and we describe the architecture and functionalities of a relevant middleware that represents a possible solution to this issue. Secondly, we propose a consensus protocol for the cooperation among network objects in performing the target application, which aims to distribute the burden of the application execution, so that resources are adequately shared. We demonstrate that, using the proposed protocol, the network converges to a solution where resources are homogeneously allocated among nodes. Performance evaluation of experiments in simulation mode and in real scenarios show that the algorithm converges with a percentage error of about 5% with respect to the optimal allocation obtainable with a centralized approach.

1. Introduction

The last few years have been involved by the technological revolution represented by the Internet of Things (IoT) [1]. The IoT vision aims to interconnect devices with different capabilities such as sensors, actuators, Radio Frequency Identification (RFID) tags, smart objects (e.g. smartphones), and servers, within the same heterogeneous network. The aim is to enable the network objects to dynamically cooperate and make their resources available, in order to reach a goal, i.e. the execution of one or more applications assigned to the network.

Available resources (such as electrical energy, memory, processing, and node capability to perform a given task) are often limited. This is the case, for example, of wireless sensor nodes, which are often battery powered, and therefore have limited energy amounts. Another example is represented by the scarce processing capabilities of RFID tags. Given the size of a distributed heterogeneous system such as the IoT network, the resource allocation issue with the aim of improving network performance is not trivial. Furthermore, IoT networks are characterised by the dynamic behaviour of their nodes. In fact, emerging applications in smart environments such as smart cities and smart homes, where IoT is preponderant, are often based on opportunistic networks and opportunistic sensing. In opportunistic networks, connections among nodes are created dynamically in an infrastructure-less way: when forwarding a message, next hops are chosen opportunistically, on the basis of their likelihood to get the message closer to its destination [2]. Opportunistic sensing is characterised by sensors that erratically sense the environment, whenever

---

* Corresponding author.
E-mail addresses: giuseppe.colistra@diee.unica.it (G. Colistra), virginia.pilloni@diee.unica.it (V. Pilloni), l.atzori@diee.unica.it (L. Atzori).

http://dx.doi.org/10.1016/j.comnet.2014.07.011

their state (such as location or user activity) matches application's requirements [3]. In such a dynamic context, with frequent and quick changes of scenario, it is not reasonable that resource allocation is accomplished in a centralized way.

To the best of authors' knowledge, there are not studies focusing on distributed resource allocation in IoT. Some past studies such as [4,5] focused on finding and allocating network resources that enable service execution. However, these works are not aimed at finding the best solution among alternative ones but they consider that only one solution is available. Accordingly, the best way to distribute the usage of resource is not their concern.

In this work, we face the challenges of the deployment of distributed applications in the IoT in terms of cooperation among objects, with the aim of distributing the burden of the execution of the application committed to the network, so that resources are adequately exploited. Since opportunistic sensing and opportunistic networks are paramount in IoT scenarios, we focus on solutions for this kind of networks.

Our contribution in this paper is twofold: (i) we first define the problem and the challenges related to resource allocation for the deployment of distributed applications in heterogeneous networks. Based on these considerations, we describe the architecture of the proposed middleware that enables the implementation of application deployment to network resources, by means of a distributed and coordinated negotiation among network objects. (ii)We then provide a distributed protocol based on the consensus algorithm proposed in [6], and we adapt it to solve the problem of resource allocation and management in IoT networks. In particular, we focus on adjusting sensing functionalities of objects so that resources are equally shared among nodes participating into the application execution. Simulation and real scenario results prove that the convergence of the consensus algorithm is quickly reached.

The rest of the paper is organised as follows. Section 2 describes the reference scenario of an opportunistic IoT network and its features. Section 3 analyses some related works and how they approach the resource allocation problem. In Section 4, the consensus model in the algorithm is introduced. Section 5 describes the protocol. Finally, Sections 6 and 7 present the algorithm performance analysis and draw conclusions, respectively.

2. The reference scenario

In the IoT, key nodes are represented by sensors, actuators, RFID tags, smart objects, and servers connected to the Internet [1], which have the most diverse characteristics and capabilities. All these types of devices need to interoperate and reconfigure in an autonomous way, in order to perform some given applications dynamically [7,8]. Other than node heterogeneity, we consider the scenarios characterized by wireless communications that exploit opportunistic networking as a way for improving cyber-physical systems pervasiveness in the environment [9,10]. Accordingly, the information are addressed, disseminated and shared within and among opportunistic communities of devices that are formed based on the movement and opportunistic contact nature of humans [11]. In this scenario, not only opportunistic communications are highly desirable but also sensing so that nodes allow their sensors to be remotely tasked on someone else's behalf, collecting and reporting sensor data on a best-effort basis when the conditions permit [12].

In this depicted scenario, it frequently happens that some nodes perform the same sensing operation, such as the measurement of the traffic in the same street, the measurement of the humidity and/or the temperature in a room, the detection of moving objects/persons in a given environment, the monitoring of the luminosity in a public square. However, not all nodes have usually the same amount of resources to be dedicated to the same tasks and the set of nodes that can cooperate in performing a given operations changes quickly as opportunistic behaviours make the scenario quite dynamic. Accordingly, groups of nodes are identified, namely, *task groups*, that perform similar and replaceable tasks. To understand the meaning of *task group*, suppose, for example, that the network is performing a temperature sensing in a specific area: only those nodes that are equipped with a temperature sensor and that are deployed within that area are included in the *task group* related to this task. These *task groups* are assigned with the relevant task by the application deployment server, which could decide which exact node should perform each needed task. Alternatively, it may leave these groups of nodes to autonomously decide how to distribute the burden of tasks among them without the need for the central server to keep the role of single physical node controller. According to the latter vision, the IoT is made of *virtual objects* (VOs) [13] which are activated by the Central Deployment Server. The VO role may be implemented by a node in the *task group* and is in charge of processing the requests generated by the central server and forwarding configuration messages to the other physical nodes (note that the virtual node may coincide with the only single physical node that is capable of implementing the required task). At this point, allocating the proper resources to the required task is a duty of the nodes in the *task group*.

Fig. 1 provides a sketch of the above described reference scenario. The central server, or a leader node, transmits the activation signal to the VO. Since the VO is responsible for keeping track of the physical nodes that belong to the same *task group* it leads, it knows which nodes the activation signal is addressed to. Therefore, it is able to forward the activation signal to the appropriate nodes, on the basis of their belonging to a determined *task group*. The aim of the algorithm explained in Section 5 is, for each node belonging to the same *task group*, to dynamically change its assignment, in order to share the effort required to perform the considered task, in terms of necessary network resources.

3. Related works

In this Section we aim at presenting how the task allocation problem has been addressed in the different contexts of relevance for the considered scenario.