Chapter 2
Internet of Things Research Challenges

Mahmoud Elkhodr
Western Sydney University, Australia

Seyed Shahrestani
Western Sydney University, Australia

Hon Cheung
Western Sydney University, Australia

ABSTRACT

The Internet of Things (IoT) promises to revolute communications on the Internet. The IoT enables numerous business opportunities in fields as diverse as e-health, smart cities, smart homes, among many others. It incorporates multiple long-range, short-range, and personal area wireless networks and technologies into the designs of IoT applications. This will result in the IoT being pervasive in many areas which raise many challenges. This chapter reviews the major research issues challenging the IoT with regard to security, privacy, and management.

INTRODUCTION

The Internet of Things (IoT) foresees the interconnection of billions of things by extending the interactions between humans and applications to a new dimension of communications via things. Rather than always interacting with the users, things will be interacting with each other autonomously by performing actions on behalf of

DOI: 10.4018/978-1-5225-0741-3.ch002

the users. Consequently, the availability of information coming from non-traditional computer devices in the digital world will, in great parts, lead to improving the quality of life. Over the next couple of years, it is predicted that the industrial value of the IoT will surpass that of the Internet 30 times over, and to be a market that is worth more than $100 billion dollars (Clendenin, 2010). On the other hand, it is estimated that there will be more than 20 billion devices connected to the Internet by 2020 (Lomas, 2009). While Cisco predicts that the number of connected devices will exceed 50 billion in 2020 (Evans, 2012). The IoT will revolute many industries and elevate communications on the Internet. The IoT provides the user with numerous services and capabilities. The obvious ones are the ability to control and monitor the physical environment remotely over the communication networks. Typical examples are the ability to close a door or receiving smoke alert notifications, and the likes, remotely over the Internet. However, the true vision of the IoT revolves around connecting networks and a group of sensors together in an intelligent and ubiquitous fashion. Thus, the IoT promises to enable numerous business opportunities in fields as diverse as e-health, smart cities, farming among many others.

The interconnection of things allows not only things to communicate with each other but also offers the opportunities of building intelligence and pervasiveness into the IoT. For instance, by connecting home appliances to the smart grid, the IoT will enable better energy consumption and water conservation. In addition to helping users in monitoring their own usage, the IoT will optimize energy demand distribution across a city and regulate the automatic consumptions of electricity and other resources. For that to happen, the IoT will need to access a vast array of data and devices, analyze the users' behaviors, and monitor occupancy and lighting conditions. It also needs to collect various sensitive information about the users, their activities and environment. This will result in the IoT being pervasive in many areas. Hence, the potentially massive number of things, their diversity, and the seamless and heterogeneous nature of communications encountered in the IoT raises many research challenges.

Many envisioned IoT applications will require the automated sharing of the users' information collected by things. This requires agreements on many applications and networks levels. How things will be identified and accessed on the Internet remains unclear. The integration of smart devices, Wireless Sensor Networks and IoT applications in one network pose numerous challenges to the traditional network and managements approaches. Additionally, the autonomous aggregation of users' information gathered by a large number of things and exchanged over various heterogeneous networks impinge on the security and privacy of the users. For this reason, the development of solutions to support security protection, management, and privacy preservations are key factors for the proliferation of the IoT. Towards this aim, this Chapter reviews some of the significant research issues challenging the