Chapter 6
Distributed Access Control for IoT Services Based on a Publish/Subscribe Paradigm

ABSTRACT

With IoT services becoming more open and covering wider areas, different IoT applications at different sites are now collaborating to realize real-time monitoring and controlling of the physical world. The use of a publish/subscribe paradigm allows IoT applications to collaborate more closely in real time and to be more flexible. This is due to the space, time, and control decoupling of the event producer and consumer, which can be used to establish an appropriate communication infrastructure. Unfortunately, a publish/subscribe-based IoT application does not know which users are consuming its data events, and consumers do not know where the events originate from. In this environment, the IoT application cannot directly control access, since interactions in the application are anonymous and indirect. To address these issues, this chapter first describes a foundation for communication between wide-area IoT services and then defines a security model supporting a data-centric methodology. Using this model, the underlying network capabilities can be integrated to help IoT applications control event access. The key concept in this access control solution is the preservation of the interaction characteristics of publish/subscribe-based IoT applications, which are both anonymous and multicast. Thus, two specific types of event are used to accomplish requests for and granting of authorization, while remaining consistent with the publish/subscribe paradigm. A policy-attachment method is used to preserve the anonymity and multicast features of the collaborating IoT applications, where policy-matching efficiency, policy privacy, and communication performance are the main points of focus. This access control scheme can also be enhanced with confidentiality.

DOI: 10.4018/978-1-5225-7622-8.ch006
INTRODUCTION

Motivation

Modern wide-area IoT applications can be viewed as an evolutionary system with greater efficiency and openness and use integrated communication technologies and computational intelligence to realise the goal of interconnection. A new communication infrastructure is needed for the delivery of coherent and real-time data in such systems; for example, in a smart grid, a fault in one transmission line can result in a chain reaction and an eventual blackout. This situation requires the visibility of the power system to be improved. If there is no overall picture of the power system and situational awareness is updated only slowly, the significance of the initial event cannot be recognised so that action can be taken to avoid the blackout. In this type of communication infrastructure, informational connections may be made using time-synchronised measurement devices such as a phasor measurement unit (PMU), a phasor data concentrator (PDU) and so on.

Some blackouts take place too quickly to allow operator intervention, and fast control and protection schemes are therefore needed to prevent the power system from reaching instability or collapse. These schemes also depend on coherent, real-time data that are delivered in an appropriate way. Furthermore, the integration of many non-carbon sources of energy, such as wind and solar power, complicates the control procedure, since these behave differently from existing generation sources and are dependent on local weather conditions. To address these issues, a smart grid requires the modernisation not only of the power system but also of its data delivery infrastructure. Time-synchronised measurement technologies should therefore be used, and microsecond-accurate data should be delivered in real time to provide coherent picture of the power system to operators, and to allow closed-loop control and broader protection.

The GridStat (Washington State University) project (Bakken et al. 2011) adopted a publish/subscribe paradigm to build a communication infrastructure in which a data consumer can express interest through a subscription without knowing who produces the data, and the data producer publishes data without knowing who subscribes to these data. This type of communication infrastructure is not aware of where the information is located, but only of which information is needed. A customer can describe her requirements based on the event type, and the infrastructure will deliver data of this type, even if the data producer did not intend to send the data to this customer. Multiple
Data Extraction from Deep Web Sites
[www.igi-global.com/chapter/data-extraction-deep-web-sites/16846?camid=4v1a](www.igi-global.com/chapter/data-extraction-deep-web-sites/16846?camid=4v1a)

Network-Based Intrusion Detection
[www.igi-global.com/chapter/network-based-intrusion-detection/16875?camid=4v1a](www.igi-global.com/chapter/network-based-intrusion-detection/16875?camid=4v1a)