Chapter 19

DEAL: A Distributed Authorization Language for Ambient Intelligence

Irini Genitsaridi
Institute of Computer Science, FORTH, Greece

Antonis Bikakis
University College London, UK

Grigoris Antoniou
Institute of Computer Science, FORTH, Greece

ABSTRACT

Authorization is an open problem in Ambient Intelligence environments. The difficulty of implementing authorization policies lies in the open and dynamic nature of such environments. The information is distributed among various heterogeneous devices that collect, process, change, and share it. Previous work presented a fully distributed approach for reasoning with conflicts in ambient intelligence systems. This paper extends previous results to address authorization issues in distributed environments. First, the authors present the formal high-level authorization language DEAL to specify access control policies in open and dynamic distributed systems. DEAL has rich expressive power by supporting negative authorization, rule priorities, hierarchical category authorization, and nonmonotonic reasoning. The authors then define the language semantics through Defeasible Logic. Finally, they demonstrate the capabilities of DEAL in a use case Ambient Intelligence scenario regarding a hospital facility.

INTRODUCTION

Ambient intelligence (AmI) is a new wave of information technology that integrates microprocessors into everyday objects in order to improve the quality of everyday life. AmI environments include heterogeneous intelligent devices that communicate by means of ad-hoc wireless networks. Each intelligent device acts as an autonomous entity that controls resources, handles requests and shares information and services with other entities. The core difference between AmI and traditional systems is the formers’ user...
centric approach. AmI systems adapt and respond to people by acknowledging their presence and gestures instead of the other way around.

Ambient Intelligence is a multidisciplinary approach as presented in Aarts (2004) and Remagnino and Foresti (2005), since it requires the convergence of many areas of Computer Science in order to fulfill its purpose. Therefore, it has introduced new research challenges in many areas, including the field of access control. The implementation of access control is vital in order to develop a secure AmI system. Each intelligent device should be able to specify access policies to the resources that it controls. However, the special characteristics of AmI environments make the specification and implementation of access control problematic.

Ambient Intelligence environments are characterized by the imperfect nature of context information. Aboud, Dey, Brown, Davies, Smith, and Steggles (1999) defined context as “any information that can be used to characterize the situation of an entity. An entity is a person, place or object that is considered relevant to the interaction between a user and application, including the user and applications themselves”. Henricksen and Indulska (2004) characterize four types of imperfect context information: unknown, ambiguous, imprecise, and erroneous. Sensor or connectivity failures (which are inevitable in wireless connections) result in situations, that not all context data is available at any time. When data about a context property comes from multiple sources, then context may become ambiguous. Imprecision is common in sensor-derived information, while erroneous context arises as a result of human or hardware errors.

Moreover, AmI environments are characterized by their open and dynamic nature. In an open and dynamic environment participating entities enter or leave the environment at random times and without prior notice. Such entities are expected to have different goals, experiences and perceptive capabilities. They may use distinct vocabularies to describe their contexts, and may even have different levels of sociality. Due the unreliable and restricted (by the range of the transmitters) wireless communications, direct communication with all entities may not always be feasible.

In this paper we study the problem of authorization, as a basic part of access control in Ambient Intelligence environments, and provide a fully distributed approach to address it. Authorization is the process of specifying an access control policy that is used to determine whether a requester, with a given valid identity, is permitted to consume a particular requested service.

We propose a formal high-level logic-based language for addressing authorization issues in AmI environments. Our work builds on our previous work on a distributed model for contextual reasoning, called Contextual Defeasible Logic (CDL) (Bikakis & Antoniou, 2010, 2011; Bikakis, Antoniou, & Hassapis, 2011). CDL is based on Defeasible Logic (Antoniou, Billington, Governatori, & Maher, 2001; Nute, 1994), which is skeptical, rule-based, and uses priorities to resolve conflicts among rules. CDL also adopts ideas from Multi-Context Systems (MCS) (Giunchiglia & Serafini, 1994). A MCS consists of a set of logical theories called contexts, and a set of inference rules (i.e., mapping rules) that enable information flow between different contexts. In CDL, the Multi-Context Systems model is enriched through defeasible rules, and priority relations that provide a preference ordering on system contexts to represent their comparative reliability. Although CDL provides a flexible approach for reasoning about context in distributed environments, it does not address authorization issues. In this work we implement an authorization language as an extension of the language of CDL in order to address the access control requirements of Ambient Intelligence systems. We emphasize on the expressive power of the language in specifying authorization policies of distributed systems.