ABSTRACT

Ubiquitous computing and ambient intelligence (or AmI) models raise the need for secured systems, due to increased heterogeneity, intelligence and dynamism. Information in such environments is managed by systems formed mostly of devices with limited capabilities. Indeed, AmI characteristics, difficult to handle by traditional computing concepts, are making the agent paradigm to gain impetus and increasing the interest of researchers and industry in this concept. However, the inherent complexity of information security is bigger in agent-based AmI systems built by gathering distributed information and services that are not under the control of a single entity, and introduce new security and privacy concerns. In fact, securing these systems requires protecting any element from every other. This paper proposes a mechanism for enhancing security and privacy while using agents in AmI environments, based on three main building blocks: verification, judgment and surveillance. Furthermore, the key idea is based on cooperation and collective decision.

Keywords: Agents, Ambient Intelligence (AmI), Attribution of Privileges, Collective Decision, Degree of Trust, Security

INTRODUCTION

According to many authors, the aim of the Ambient Intelligence environment is to provide a context aware system, using unobtrusive computing devices, which - in their vision - will improve the quality of people’s lives by acknowledging their needs, requirements and preferences and thus acting in some way on their behalf. Additionally, pervasive computing should enable immediate access to information and services anywhere, anytime (Schreurs, Hildebrand, Gasson, & Warwick, 2004).

We must note that in AmI scenarios the computational infrastructure is composed of a very large number of computing mobile devices, called AmI devices, having heterogeneous capabilities, autonomy, intelligence and under the control of different owners (Weiser, 1991; Augusto, 2008).
These characteristics introduce the necessity to use agent paradigm (Ferber, 1995), having a set of abilities which allow them to cover several needs for AmI environments.

They have already been successfully applied to several AmI scenarios such as education, culture, entertainment, medical domain, robotics and home. In this sense, agents are called ambient agents.

For example, Alzheimer multi-agent system (Tapia, 2010) aimed at enhancing the assistance and healthcare for Alzheimer patients. Tele-monitoring Homecare is a multi-agent system designed to enhance remote healthcare of dependent people at their homes (Alonso, Saavedra, Tapia & Corchado, 2009).

Note that in all these systems, agents are attached and embedded in an AmI device, so called ambient agents.

These devices are increasingly used to store sensitive personal information about private life, health or financial data used for mobile banking.

Consequently, the success of AmI systems based on ambient agents, will depend on how privacy and other rights of individuals can be protected and how individuals can come to trust the intelligent world that surrounds them and through which they move? (Stajano, 2010)

Moreover, new AmI applications make AmI device and ambient agent embedded in it, an enticing target for attackers, malicious software and mischievous agents.

Additionally, the most obvious challenge for developing security mechanisms for mobile AmI devices is their constrained resources. Unlike their desktop brethren, AmI devices have strict resource constraints in both computational and power capabilities due to their mobility and small size. They are interconnected by wireless or wired networks, working together and cooperating towards the resolution of tasks (Roovers & Aarts, 2003).

Therefore, while complex detection algorithms may scale in standard non constrained desktop environments, they can be less effective in resource-constrained mobile environments (Oberheide & Jahanian, 2010).

In this paper we present a contribution to provide a secure environment for ambient agents’ group in AmI computing scenarios, by taking in to consideration the new required challenges.

The rest of the paper is structured as follows: the next section provides an overview of relevant related work. The following section describes the proposed protocol and architecture of agents. In the section after that, we propose an implementation using JADE platform and we give some experiments results. Finally, the last section summarizes the paper and describes some ongoing works.

BACKGROUND AND RELATED WORK

Protection works proposed for classical multi agent systems are divided into two broad classes. The first protection mechanisms are oriented to the protection of the host system against malicious agents.

Other mechanisms are oriented towards protecting agents against malicious agents. In the context of AmI environments, we consider that agents are fixed into mobile devices. So, in this section we will focus the protection of agents against malicious agents or entities. Then, we will discuss the insufficiency of these approaches for ambient agents groups.

Sandboxing (Gong, Mueller, Prafullchandra, & Schemers, 1997) is an original and popular security model provided by Java. It is based on the creation of a secure execution environment for non-trusted software. In the agent world, a sandbox is a container that limits, or reduces, the level of access its agents have and provides mechanisms to control the interaction among them.

The limitation of this approach is easily recognizable: it can provide security only at the cost of unduly restricting the functionality of mobile code (e.g., the code is not permitted to access any files). The sandbox model has been subsequently extended in Java 2 (Gong
Utilisation of Case-Based Reasoning for Semantic Web Services Composition
www.igi-global.com/article/utilisation-case-based-reasoning-semantic/2445?camid=4v1a