Computer Standards & Interfaces 31 (2009) 913–930

Contents lists available at ScienceDirect

Computer Standards & Interfaces

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

An extended JADE-S based framework for developing secure Multi-Agent Systems

Salvatore Vitabile [a,*], Vincenzo Conti [b], Carmelo Militello [b], Filippo Sorbello [b]

[a] Dipartimento di Biotecnologie Mediche e Medicina Legale, Università di Palermo, Via del Vespro, 129-90127, Palermo, Italy
[b] Dipartimento di Ingegneria Informatica,Università di Palermo,Viale delle Scienze, Ed. 6-90128, Palermo, Italy

ARTICLE INFO

Available online 7 April 2008

Keywords:
Multi-Agent Systems (MASs)
MAS Security
JADE-S
Biometric Authentication
FPGA Prototyping
e-Banking System

ABSTRACT

Agent communities are self-organized virtual spaces consisting of a large number of agents and their dynamic environments. Within a community, agents group together offering special e-services for effective, reliable, and mutual benefits. Usually, an agent community is composed of specialized agents performing one or more tasks in a single domain/sub-domain, or in highly intersecting domains. However, secure Multi-Agent Systems require severe mechanisms in order to prevent malicious attacks. Several limits affect exiting secure agents platform, such as the lack of a strong authentication system, the lack of a flexible distributed mechanism for access control and the lack of a system for storing past behaviors of agent/user. Biometric owner agents authentication, agent/users policies to regulate agent's behavior and actions, and agent/users reputation level to select trusted agents can be used to overcome the above limits and enhance the level of security for these applications. In this paper an extended JADE-S based framework for developing secure Multi-Agent Systems is proposed. The framework functionalities are extended by self-contained FPGA biometric sensors providing secure and fast user authentication service. Each agent owner, by means of biometric authentication, acquires his/her own X.509v3 digital certificate. Policy files and a flexible, fast distributed Access Control Mechanism can regulate behavior and actions of any users/agent inside the platform. In addition, a mechanism based on the agent reputation is used: reputation is an attribute associated to each owner and/or agent on the basis of its past behavior and integrity. In order to prove the feasibility of the proposed framework, we have developed a multi-agent e-Banking system. System goal deals with e-Banking services such as bank account statements, account transactions and so on. In the paper, the experimental features of the biometric self-contained sensors are also outlined.

1. Introduction

Multi-Agent Systems (MASs) are becoming very popular and used in several domains. However, a focal service deals both with the security risks associated to these systems and the related counter-measures for designing secure MASs [1]. Due their flexibility, scalability and interoperability, secure MASs can be used in several distributed domains, such as e-Banking, e-Commerce, where the treatment of personal information is a critical issue. Critical problems and limits concerning exiting secure infrastructures are:

- the lack of a strong authentication system to solder agent and its owner;
- the lack of a security mechanisms for users acting as client (requiring a service);
- the lack of a flexible distributed Access Control Mechanism;
- the lack of a system for storing past agent/user behaviors (agent reputation recording).

As all distributed applications, MASs need to provide distributed owner access [44], rather than a single access-point: embedded self-contained authentication sensor represents the natural solution of this problem. The main objective of this approach is to overcome some limits of the conventional software biometric recognition systems, such as user interaction speed and resistance to attacks related to transmission and management of biometric data. On the other hand, the Agentcities Security Working Group has defined a set of security requirements identified for multiple agent platforms active in open distributed multi-domain networks. Among the application driven requirements, user authentication based on both invasive and non-invasive biometric features is suggested [2].

In this paper, an extended JADE-S based framework integrating biometrics features for the owner authentication, a flexible, fast distributed Access Control Mechanism, and a distributed agent/users reputation system for selecting trusted agents is proposed. Due to its versatility, the framework simplifies the development of multi-secure agent applications integrating the described countermeasures in order to prevent security attacks.

Using biometric features, an agent owner could be identified through his/her physiological or behavioral characteristic. So a MAS biometric-based authentication systems can be used to increase the

* Corresponding author.
E-mail addresses: vitabile@unipa.it (S. Vitabile), conti@unipa.it (V. Conti), militello@unipa.it (C. Militello), sorbello@unipa.it (F. Sorbello).

0920-5489/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2008.03.017

security level of the owner authentication process, since the user is identified considering "who he is", rather than by "what he has" (e.g., an ID card) or "what he remembers" (e.g., a password) [20,43].

Each agent, after the biometric authentication of its owner, obtains its own X.509v3 digital certificate. A mobile agent proves its identity and integrity through its Identity Certificate, signed by a Certification Authority. Digitally-signed certificates with biometric information are provided and checked by the platform Certification Authority in order to grant agent/owner rights.

The Certification Authority could also check against the owner reputation level before granting/denying permission to perform certain actions. Agent rights and owner reputations are strictly related: a network authority can temporarily or permanently suspend or revoke digital certificates to untrusted agents/users. A reputation-based mechanism is applied: reputation is an attribute associated to the agent on the basis of its past behavior and integrity. A reputation system is aimed at publishing information about trusted and untrusted agents, encouraging agents to have trusted behaviors and discouraging untrusted behaviors.

The mechanism of reputation, whose score is dynamic, allows to communicate and/or to delegate agents with high level of reputation with the purpose to carry forward the trusted and secure transactions.

A dynamic policy to regulate agent behavior and actions, including permission, rights, and ties, can be included in MASs. The system, through the biometric authentication, X.509v3 digital certificates and the dynamic policy file, monitors the operations of any users/agent inside the platform. The Certification Authority can change the agent reputation score and lastly remove, through the revocation of the file of policy, the possibility of any action in the system.

The effectiveness of the proposed system has been proven through a multi-agent based e-Banking system, since these systems require high security mechanisms for both agents and platform. A distributed e-Banking system provides a lot of on-line services to registered users. System security features are a secure agent owner access, flexible and ubiquitous access system, a policy to regulate users/agents behavior and action and a reputation score associated to each agent on the basis of its past behavior, its correctness, and its reliability.

The developed multi-agent system is composed of four categories of agents, each of one having its specific functions. The *Interface Agent* is the interface between the user and the distributed e-Banking system. The agent gets queries from users and returns the transaction results. The *Banker Agents* are a collection of agent able to execute simple tasks on bank repositories, such as find a bank account or give out an account statement. The *Resolver Agent* is able to migrate or clone itself on each repository of the banking network. Each request, coming from the Interface Agent, will be evaluated by this agent. The agent has an intelligent behavior, based on Soft Computing based methods. The agent is able to act directly on network repositories, on the Banker Agents extracted information, to delegate a received task to the apposite Banker Agent. Finally, the *BioUpdater Agent* contains the updated biometric descriptors of all the enrolled users and clones itself on each bank host to update the self-contained biometric sensor.

The paper has been structured as follows. In Section 2 an overview of the most used secure MASs is reported. Section 3 gives an overview about trust and security, while in Section 4 the proposed framework is described. In Section 5 system functionalities and the implemented e-Banking system are described. Finally, Section 6 reports the conclusion of the current work.

2. Secure Multi-Agent Systems

Mobile agents offer a greater opportunity for abuse and misuse, broadening the scale of threats significantly. New computer security threats, related to the mobile agent paradigm, are due to the fact that, contrary to the "conventional" situation where the application owner and the system operator are the same, the agent's owner and system's operator could be different.

An agent comprises code and state information needed to carry out computations or applications. Mobility allows an agent to move or hop among different agent platforms. The agent platform provides the computational environment in which an agent operates. The platform where an agent originates is referred to as the home platform, and normally is the most trusted environment for the agent. One or more hosts may comprise an agent platform, and an agent platform may support multiple locations or meeting places where agents can interact [1]. The authentication process establishes the identity of each owner and, consequently, of each agent. A policy, based on the previous identity, can determine the access level of an agent in electronic distributed systems (i.e., e-Banking system, e-Business system, etc.), the permission to access certain resources or perform certain tasks [2].

2.1. The JADE-S platform

The Foundation for Intelligent Physical Agents (FIPA) developed specifications for the implementation of Multi-Agent Systems [41]. The physical infrastructure in which agents can be deployed consists of: the hardware platforms, the operating system, the agent support software, the FIPA agent management components (the Directory Facilitator (DF), the Agent Management System (AMS), the Agent Communication Channel (ACC), and the Internal Platform Message Transport). According to the FIPA specifications, there must be at least one DF agent per platform. An agent can register its services in the DF. The DF supplies the Yellow Pages (YP) service and the agent can submit a query to the DF in order to find the required service. Furthermore, the DF maintains an accurate, complete, and up-to-date list of agents. The AMS is unique to the platform and is responsible for managing the agent creation, deletion and migration. The ACC routes messages between agents within the agent platform to agent's resident on other agent platforms.

JADE (*Java Agent DEvelopment framework*) is a FIPA compliant software framework fully implemented in the Java language, which simplifies the implementation of Multi-Agent Systems. The platform can be seen as a middleware (Fig. 1) providing a set of useful tools that support the debugging and deployment phase [3,4,6].

JADE-S is formed by the combination of the standard version of JADE with the JADE security plug-in [5]. JADE-S includes security features such as user/agent authentication, authorization and secure

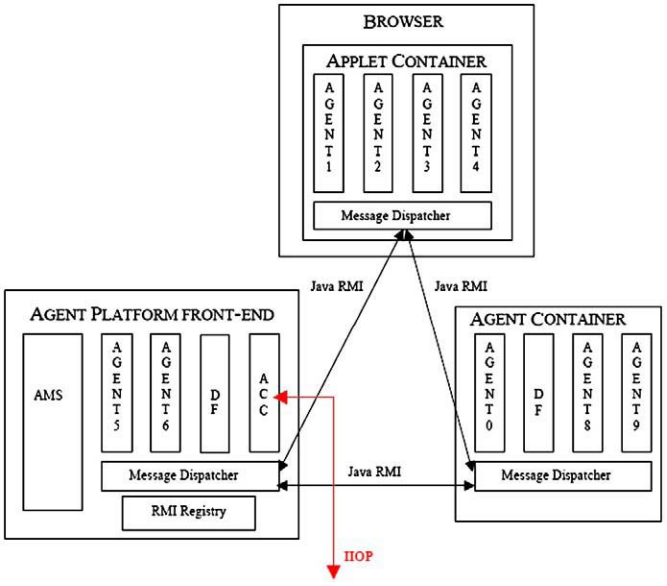

Fig. 1. Software architecture of one JADE agent platform ([3]).