Track C

Session I: Friday / 09.00 – 10.45

Security I

Talk-Ci.1: "A Fingerprint Based Authentication System for the JADE-S Platform" Salvatore Vitabile, Vincenzo Conti, Giovanni Pilato, Filippo Sorbello

The Jade-S platform authentication requires username and password for users and/or component authentication. The platform policy establishes what kind of actions an user can perform. In this work an enhanced access system for the JADE-S (Java Agent DEvelopment Framework Security) is presented. The proposed access system requires user fingerprint in addition to the standard items required by JADE-S. Consequently, a new authentication agent that is able to deal with fingerprint sensor and with the related authentication process has been designed. The acquired fingerprint image is processed with noise immune algorithms based on its micro characteristics and a matching is performed between the on-line acquired fingerprint image and the related database image. The authentication agent performs the user verification task in three main phases: fingerprint pre-processing, fingerprint minutiae extraction and fingerprint matching. The pre-processing phase goal is the binarization of the acquired fingerprint image. Image binarization is performed using an adaptive threshold depending on the median of the image energy histogram. In the second phase the fingerprint meanly features, called minutiae, are extracted. The fingerprint matching phase is used to verify the acquired fingerprint and it is based on a new intersection operator, that is an extension of the Tanimoto distance, in order to enhance system performances with noisy, translation and/or rotation problems. The authentication system has been successfully tested implementing a Jade-S platform with the new designed agent. For each user, the authentication process is performed using the username, password and fingerprint acquired through the SecuGen Eyed Hamster sensor.

Talk-Ci.2: "Threats and security safeguards in a Multi-agent System Medical Applications" David Cabanillas, Steven Willmott, Ulises Cortés

This talk describes threats and safeguards over an agent application. Areas where the security has a considerable importance cover a wide range of applications. In our case we are focused eHealth which is an area where terms such as privacy and trust have a great importance. We have focused about this because we believe that health applications could make important things in our society. We hope however but own conclusions are applicable in the rest of the areas where security is demanded.

Talk-Ci.3: "An Incentive Compatible Reputation Service", Radu Jurca, Boi Faltings

Traditional centralised approaches to security are difficult to apply to large, distributed, multi-agent systems (MAS). Developing a notion of trust that is based on the reputation of agents can provide a softer notion of security that is sufficient for many MAS applications. However, designing a reliable and "trustworthy" reputation mechanism is not a trivial problem. In this paper, we present an incentive-compatible reputation mechanism (i.e it is rational for agents to truthfully share the reputation information they have acquired in their past experience) based on a side-payment scheme organised through a set of broker agents, called R-agents. A cryptographic mechanism is used to achieve a tight bounding between the identity and the reputation of the agents in order to provide non-manipulation guarantees of the mechanism.

Ci: Status report on SOA & Security requirements documents

Session II: Friday / 11.15 – 13.00

Security II

Talk-Cii.1: "Towards a collaborative filtering method in an open world", Miquel Montaner, Beatriz López, Silvana Aciar, Esteve del Acebo

One of the most emergent popular services developed for a city is restaurant recommenders. Several approaches are followed, from individual recommender agents to distributed systems in which an agent for each restaurant is implemented. Our approach is also a distributed approach but regarding the collaborative recommendations in an open environment: users profiles are not kept in a server but distributed in each individual user computer. A hybrid procedure of collaborative and content-based filtering is defined, in which a trust mechanism has been developed. When an agent has a lack of information situation in order to recommend some item to the user, it looks for the opinion on the item to other trustworthy agents. Trust, then, it is not due to reliability issues, but due to preference similarity among users. Similarity is not based on profile exchange but on an opinion that comes from a question-answering process between agents, keeping user data on private. In order to achieve our objective in a open environment as Agentcities, we have deployed a

Multi Agent system upon the JADE platform. Then, our restaurant recommender service consists of service agents and personal agents. Service agents offer information about restaurants and the personal agents (named restaurant server agent and personal agent facilitator, correspondingly). Personal agents are in charge of recommending restaurants to their users based on both, information on restaurants and interaction with other friendly personal agents. Personal agents interact with the restaurant server agent in order to know about the restaurants, the personal agent facilitator agent in order to know about other personal agents in the system, and the personal agents in order to find similar users and take advantage of their opinions and advice. All agents are currently available through Agentcities at http://arlab.udg.es/, and the system developed, GenialChef is registered on the Agentcities competition.

Talk-Cii.2: "Self-Organisation Mechanims Inspired from Natural Life to Build an Intrusion Detection and Response System", Noria Foukia

Today, the security community is in search of novel solutions to achieve efficient responses to intrusions. This is particularly needed because attackers intervene in an automated way, at computer speed. There is also a need to respond according to the nature of the detected attack. That is why Intrusion Detection Systems (IDS) and Intrusion Response Systems (IRS) have to cooperate and work in parallel. To this end, it is more efficient to design the IRS in function of the IDS. The IDS and the IRS are designed using Mobile Agents (MAs) in quite similar ways, since both maps the behaviour of natural systems: 1) For the detection, the human natural immune system provides a source of inspiration for today`s computer security when building IDSs, because the immune systems evolves many interesting mechanisms to defend our body against external attacks and aggressions. Defenders in the body are auto-organised to recognize unsafe sequences of peptides (the ``non-selfs``) emerging from the surface of infested cells. 2) For the response, we also took our inspiration from a social insects paradigm, namely the collective behaviour emerging from self-organized foraging ants. This behaviour expresses the way ants gather food collectively: they use an indirect communication mechanism where each ant`s motion is influenced by a chemical information (called pheromone) deposited by the other ants in the environment. Our IRS maps the collective behaviour of a population of foraging ants, using MA technology and an electronic version of pheromone. The talk shows how we combine both mechanisms to build our IDRS. This IDRS is based on a social insects paradigm to trace the source back to where the intrusion alert was generated. We specially study and describe the tuning of such a mechanism, to allow an effective scheme for intrusion response. We particularly stress the design of our IDRS and present some simulations and implementation results to demonstrate its efficiency.

Cii: Discussion - Impact of the security requirements / Framework 6 project proposals

Session III: Friday / 14.00 – 15.45

Engineering Self Organising Applications I

Talk-Ciii.1: "An agent based architecture for robotic vision systems" Ignazio Infantino, Massimo Cossentino, Antonio Chella

A comprehensive approach to the design and implementation of multi-robots cooperative systems is described. It focuses on a design process that uses the Unified Modelling Language and on a detailed ontology description with the goal of sharing the knowledge on environments that robots can acquire through the use of their vision sub-system. We base the implementation of our robotics vision system on agents inserted in a generic multi-level architectures. The first objective of this work is to provide a framework to perform a rigorous agent-based design process for scenarios where many robots are involved in different operations. Then we introduce a system for describing, upgrading and sharing knowledge about operating environments of a cooperative robot fleet. As a consequence we design a multi-level, agent-based vision architecture that takes advantage of the distribution over several different robots. The proposed multilevel architecture is based on various agents grouped in classes that have different level of knowledge: low sensorial level (Hardware Agents), sub-symbolic level (Procedural Agents and Services Agents), high level (Symbolic agent). In this structure it's possible to devise three main components: the perception, which is responsible to map the stream of raw data in a symbolic form, that in turn is provided to the cognitive component where the symbolic data computation and, in general, deliberative behaviours of the system are located. The cognitive part can also support perception with some hints aimed to refine the perceptive process, and focus the attention on those external stimuli that are judged to be more useful for the current task completion. The third component is the actuation one, which communicates with the other two, in order to drive the robot hardware during perception tasks, and in attention focusing. The perception-action link allows also reactive behaviours. All the agents can be located on