The world of autonomous distributed systems

Frances Brazier

IIDS group, CS Department,
Vrije Universiteit Amsterdam
de Boelelaan 1081a
1081 HV Amsterdam
The Netherlands
frances@cs.vu.nl

Todays world is dynamic, distributed and connected in time, space and tasks. Systems, both human and automated, interact continuously in highly dynamic environments. Some connections are relatively stable, others change very frequently, as systems and their needs change. Virtual organisations of autonomous systems are formed/emerge on the basis of characteristics such as availability, reliability, interests. Similarity, difference and/or other measures are the basis for evolving formations of organisations.

Different paradigms for distributed autonomous system development exist: p2p systems, the Grid, Autonomic Computing, Service Oriented Systems, Ambient Systems, to Multi-agent systems. Load balancing, crisis management, swarm applications, supply change management, energy management, data center management, traffic management, recommender systems, are examples of domains in which one or more of these approaches to distributed autonomous system design have been applied.

From the perspective of the users, as participants in such distributed systems, the precise technology is not of importance. The implications of the use of the technology is. This paper addresses a number of the issues shared by these paradigms and identifies a need for a framework for an understanding of the implications of the deployment of autonomous systems from the perspective of the human user..

1 Autonomous systems the underlying technology

In most of the paradigms for distributed autonomous systems, autonomous systems have some implicit or explicit knowledge of the characteristics of their owner or the organisation they represent, of the tasks they pursue (or goals) , of their own reasoning ability, of other systems characteristics and roles in relation to their own. Autonomous systems also have some knowledge of trust

relationships either implicitly or explicitly, of interaction/negotiation options, and of policies with respect to information sharing. Knowledge of their role in relation to other such systems is also often explicit.

The autonomous systems in virtual organisations, are often physically distributed and represent heterogeneous entities/institutes/organisations with different levels of accessibility, authorisation, and authentication. The can also change over time: systems come and go, as do connections. Most paradigms support both *uncoordinated* group formation , based solely on the individual systems initiative, and *coordinated* formation as the result of local management assigned to a coordinator within a virtual organisation.

In all of these paradigms interaction between systems can be *structured or unstructured, secure or not secure* .

Within the p2p paradigm, for example, interaction between peers, can be completely unstructured (eg flooding) or it can be structured (eg dht), it can be completely uncoordinated or coordinated (eg super peers), message passing can secure or not, depending on the design choices made. Characteristic of the p2p paradigm is scalability as a design criterion, thus the aim to limit the amount of information exchanged (note that this is not the same as the number of messages).

Within the Multi-Agent System paradigm, another example, the same variation with respect to structure, coordination and security is possible: interaction between agents can be structured (following eg FIPA interaction patterns) or not, can be coordinated (eg by a mediator agent) or uncoordinated, and interaction can be secure (eg JADE-S) or not.

As the paradigms can provide the same functionality there is no real reason for a user to need to know which paradigm is used. The user is interested in the options a technology provides to provide transparency.

2 User perspective a need for transparency

Transparency is a necessary condition for user acceptance of autonomous systems: transparency of system use (eg the interface), transparency of task performance, but also transparency of responsibility and liability. Integrity of individual systems (both the underlying supportive middleware and the autonomous systems themselves) and integrity of interaction between autonomous systems, are important. Guaranteeing integrity comes at a cost. A user needs to understand the balance and the risks taken in relation to the technology chosen. The same thing holds for confidentiality of information. In most cases confidentiality is of importance and needs to be guaranteed.

For the Courts of Law, for example, for which a distributed multi-agent prototype system is currently being developed for distributed management of digital dossiers for criminal offenses, supported by the Public Prosecution, complete transparency and traceability is mandatory. The advantages of a distributed digital dossier in a physically distributed environment for the digitali-

sation of digital dossiers for criminal records, in which information is provided by heterogeneous entities/institutes/organisations with different levels of accessibility, authorisation, authentication, lies primarily in the timeliness of the data involved, consistency, correctness and efficiency. Transparency and complete traceability are very strong requirements for the virtual organization. Interaction within this well-defined trusted virtual organization is necessarily well-structured, coordinated and secure. Authorised users interact with the autonomous systems representing their own organizations. Figure 1 illustrates the interactions involved.

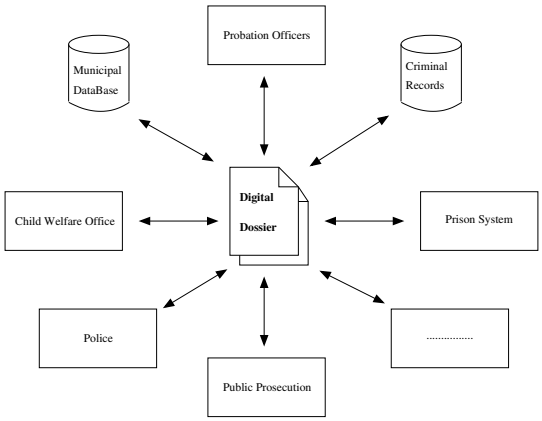

Fig. 1. Interaction with the Digital Dossier as used at a Court of Law

In other situations, such as, for example, mediated resource allocation, users interact with trusted mediators representing (virtual) organizations of resource providers. Users will want to be able to verify that all interaction between themselves and a mediator are confidential and securely logged for future reference if needed. A user does not, however, necessarily need to know about the underlying system on which offers made by a mediator are based. A user may, however, have the right to know why a request is, for example, is not honoured. To this purpose a mediator will need to be able to provide a rationale based on its own logs of interaction with the providers in its virtual organisation. Figures 2 and 3 illustrate two different virtual organisations: a well-structured, coordinated architecture, and an emergent, uncoordinated organisation, for which these logs will be needed.

An example of a virtual organisation of distributed autonomous systems for which different rules hold are open movie recommendation systems. Recommendation systems are based on user preferences and similarities. Users need to know that the value of recommendations depends on the trustworthiness of other usersdata, and that the algorithms deployed do not guarantee

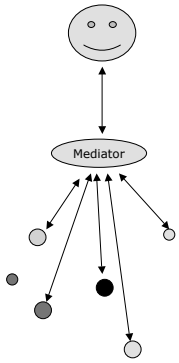

Fig. 2. A well-structured, coordinated virtual organisation

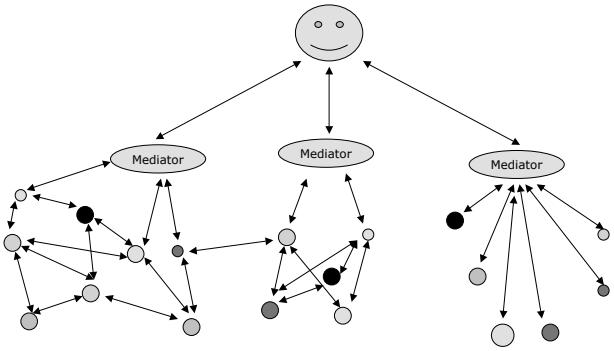

Fig. 3. An emergent, uncoordinated virtual organisation

successful recommendations. Insight in the risks and cost involved in this example, is transparent. Figure 4 depicts the users role in a dynamic virtual organisation as one of many.

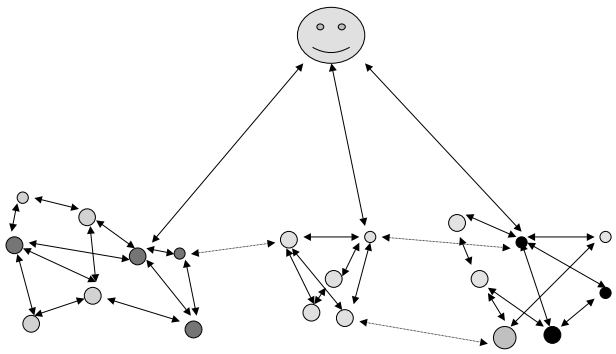

Fig. 4. The user's role in a dynamic virtual organisation

3 Discussion

For users to accept and use distributed autonomous systems, transparency is mandatory. Confidentiality, integrity, responsibilities and liabilities need to be transparent, as do the technological, legal and social implications of system failure. Our current research addresses these issues together with the development of technology to support secure and dedicated technology to support transparency in distributed autonomous systems. Technology to support coordinated and uncoordinated virtual organisations with structured and unstructured interaction patterns providing security mechanisms for confidentiality.

Acknowledgments

The author is grateful to the IIDS group and Martijn Warnier, in particular, for their contributions to this paper. The author is also grateful to Stichting NLnet, the NWO Token project and the BSIK-ICIS project for financial support.