13

AN OPERATIONAL AND SECURE MOBILE-AGENT BASED SYSTEM FOR BUSINESS PROCESS RECONSTRUCTION

Hervé Mathieu, Frédérique Biennier
Laboratoire Prisma
INSA de Lyon, Villeurbanne - FRANCE
[herve.mathieu;frederique.biennier]@insa-lyon.fr

To improve process organisations management, enterprise models should be adjusted to fit the current organisation. Moreover, infrastructure optimisation has to take into account the way it will be used. Due to these requirements, we propose to couple the Business Processes (BP) description to the infrastructure description. By this way, pro-active management on the infrastructure equipment can be implemented and reporting data can be used to rebuild the current BP execution. Due to the information diversity, we propose to implement such an Organisation Management System (OMS) thanks to a mobile agent framework. Experiments presenting how collaboration practices can be extracted from network management data bring to light the interest of such architecture.

1. INTRODUCTION

In order to improve a Virtual Organisation (VO) efficiency and to take into account contractual constraints, well-formalised inter-enterprises Business Processes (BP) have to be defined. Depending on the VO planned duration, several decision levels can be concerned by the inter-enterprise BP modelling process (strategic, tactical, operational). Often set a priori, these process models can also be used to identify efficiently problems areas to avoid to penalise the whole VO. Nevertheless, all the shared processes may not be known a priori: ad hoc workflow system can also be used to test and implement new processes. Consequently, a posteriori BP extraction process from reporting log files can be implemented. Moreover, BP descriptions can also be adjusted by taking into account all the available reporting data including those extracted from the infrastructure management systems (applications, servers, network…).

In this paper, we describe how information coming from infrastructure management systems can be coupled to the BP description to improve both a pro-active management of the infrastructure and to rebuild real BP. To support such an "organisation management system" (OMS), we propose to use a mobile agent

framework so that different kinds of data can be collected and analysed in a common framework. Experiments on collaborative practices recognition are presented to bring to light the interest of this approach.

2. BP REENGINEERING IN HIGHLY DISTRIBUTED SYSTEMS

In order to fit the reactivity, flexibility and adaptation requirements involved in Collaborative Business organisations, the VO management infrastructure should respect the different partners autonomy and be implemented in a distributed way (so that partners management systems can be added or removed easily). Such an organisation improve also the system isolation capability: in case of troubles, the problem has to be efficiently located and isolated in order to avoid to penalise the global organisation. Moreover, contractual constraints lead to well-defined inter-enterprise relationships formalisation.

Describing a snapshot at time ***t*** of the organisation, enterprise process models integrate both the enterprise organisation description AND the process description. Nevertheless, the reduced duration and the potential evolution of VO (particularly, collaboration strategies can evolve quickly) increase the need of more reactive modelling processes. To make the Business Process models fit the real ones, as well as to improve the organisation's structure, a continuous BP Reengineering (BPR) process can be done. According to (Hammer and Champy, 1993), BP reengineering is "the fundamental rethinking and radical redesign of business processes to achieve dramatic improvements in critical, contemporary measures of performance, such as cost, quality, service and speed". Such BP design can be achieved thanks to:

- **A modelling oriented process:** It consists in defining BP models and the information flows they request so that both "data driven" process organisation (Agerwala, 1982) or "task driven" organisation can be set. In this last case, processes can be described thanks to transitions, oriented graphs (Hwang and Yang, 2002) and Petri Nets.
- **A continuous "rebuilding" process:** Based on reporting data analysis (access control systems, log files…) such processes are well adapted to describe a posteriori ad-hoc workflow and may be use to deduce the exact workflow organisation from the use (Maruster et al., 2002). Nevertheless, this approach involves to define a consistent security policy so that access rights can be established a priori.

This last approach relates BP to "signatures" left on infrastructure equipment (software and hardware). Consequently, BP re-building involves first to collect and interpret data from the infrastructure management systems and then to recognise parts of signature extracted from the different management systems. In order to improve such processes, multiple sources reporting concepts have to be used.

Concepts from Intrusion Detection, taken from the computer-network security field, efficiently handle that kind of problems. Most of classical Intrusion Detection Systems (IDS) like SNORT (Caswell & al., 2003), are based on the attack signature detection paradigm. Designed to detect a particular sequence of commands (representing a kind of fingerprint), these systems identify a virus or a worm thanks

to its "fingerprint". Nevertheless, these approaches are quite empirical and are only efficient with well-known signatures. A novel approach consists in detecting attacks which may not be known yet thanks to concepts coming from immunology. Immune systems use protection mechanisms which suggest ways to improve computer security (Forrest, Hofmeyr, and Somayaji, 1997). A similar approach can be used for BP adjustment : theoretical workflow can be used as a knowledge base to guide the infrastructure tuning and to control the information extraction from the raw infrastructure data mine so that real BP can be identified. Then, once the reverse engineering of BP and workflow is achieved, it is possible to create a strong interaction between real workflow and theoretical workflow to adjust classical enterprise models (Figure 1).

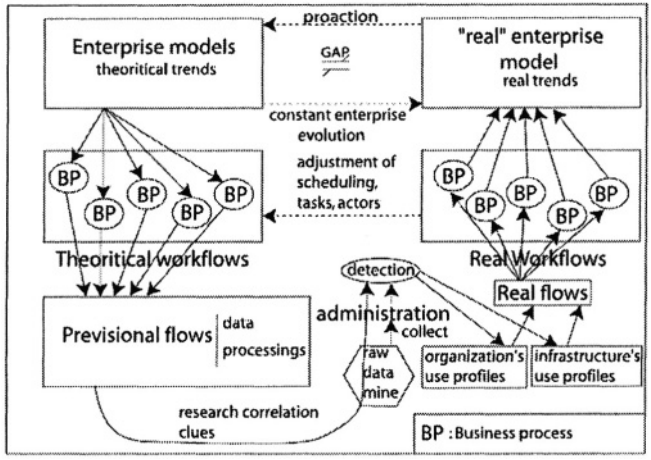

Figure 1 – Enterprise models adaptation through BP and reengineering

3. IMPLEMENTATION OF THE OMS

Due to the VO limited duration and potential evolutions, the organisation management system has to be light, flexible, and reactive. Moreover, this framework must integrate a multi-system data collection process and has to support the detection abilities diversity (i.e. inexact pattern matching strategies and reactivity towards unknown patterns). Those constraints lead us to organise the OMS framework on a mobile agent architecture. Using mobile agents for workflow management has been already explored (Lee and Shepherdson, 2003; Suh, Namgoong, Yoo and Lee, 2001), but the proposed models were not implemented, due to the lack of maturity of mobile agent technology. Flexible, well adapted to the unstable nature of a distributed environment (fault tolerance, distributed processing...) (Harrison, Chess, and Kerschenbaum, 1997), mobile agents allow a highly-distributed detection. Such architectures have also been used successfully in the communication network management field, quite similar to our BP reporting problem.

Our platform consists in reactive mobile agents (used to collect data and to modify parameters on infrastructure equipment) and area servers (used to manage agents, to analyse collected data and to exchange consistent information with other servers). Launched from the central server, a mobile agent is designed to support one particular task (raw parameter collection, configuration modification or more complex operation as log-parsing), to move from one equipment to another before going back to the central server, with collected data which are then analysed (figure 2). We expect the emergence of interesting properties from those simple operations happening everywhere on the network. Such an approach already showed its efficiency for network routing (Caro and Dorigo, 1998).

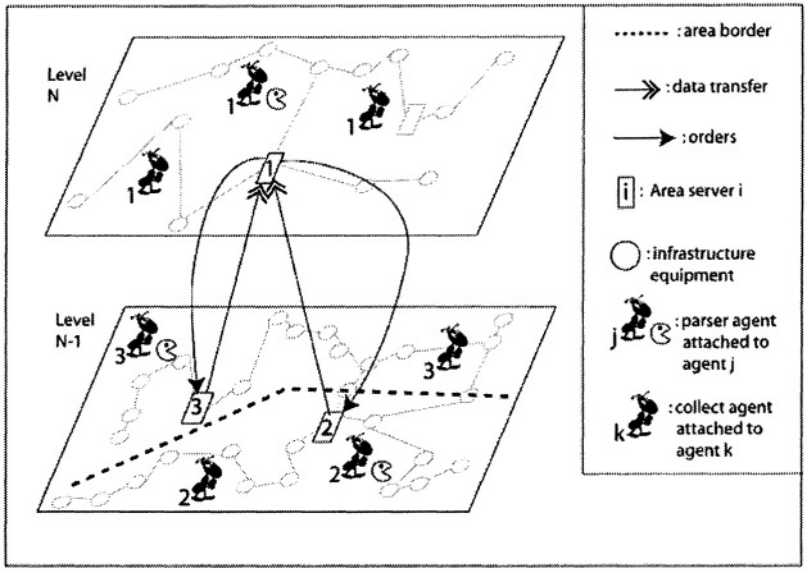

Figure 2 – Global architecture of the mobile-agent framework

3.1. Securing the mobile-agent platform

Due to the task they have to process (configuration parameter collection or update log-parsing, access control and password file manipulation…), our mobile agent framework has to pay a particular attention to security requirements in order to limit security hole introduction in the different partners infrastructure. Moreover, due to the heterogeneity and diverging security policies used by the different partners involved in a VO, the organisation management system has also to be protected "by itself" against potential threats coming form one of the partner infrastructure. As mobile agent platforms are mostly used in a protected environment (Chou, Shen and Kao, 2004), i.e. a secured network including firewalls, cryptographic features…(Garfinkel and Spafford, 2003), such platforms do not integrate natively security features. Security mechanisms for mobile agents applications have already been proposed (Rabelo, Whangham and Schmidt, 2003) but such an infrastructure still needs improvements.

As far as mobile agent framework security is concerned, two main points should be taken into account (Lange and Oshima, 1998): hosts security should not be compromised by malicious agents whereas agents must be protected against malicious hosts. Java security mechanisms illustrates this kind of technologies (use of sandbox, code signatures…). Nevertheless, it remains impossible to protect a mobile agent against a malicious host unless there is on each host specific hardware devices which can be trusted. Moreover, there is no generic solution adapted for a general use of this kind of technology (Posegga J. and Karjoth, 2000). Available technologies, such as protected memory mechanisms or advanced cryptography fit only parts of security requirements. By now, these mobile agents architectures lack of global concepts dealing with the different facets of mobile agent security.

To secure our mobile-agent framework, we developed a security architecture based on the Kerberos architecture (IETF, 1993). In this architecture, each host is related to an "area server", in charge of both launching mobile agents and authenticating hosts inside its area (similar to a KDC). Then, each hosts owns a specific "session key". This session key is also known by the area server and allows a safe transmission of the agents. The pre-requisite of such a security architecture are first that each host is known by the area server at the initialisation of the system and then that each host is trusted and will not tamper the mobile agent code in any way. Provided the fulfilment of these prerequisites, this architecture can be used to protect efficiently agents performing a simple round trip (figure 3). Then multi-layered encryption is used to protect agents performing complex itineraries (figure 4).

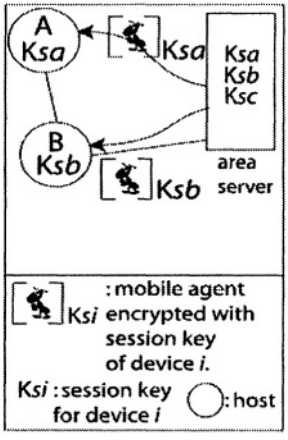

Figure 3 – Mobile-agent security Architecture

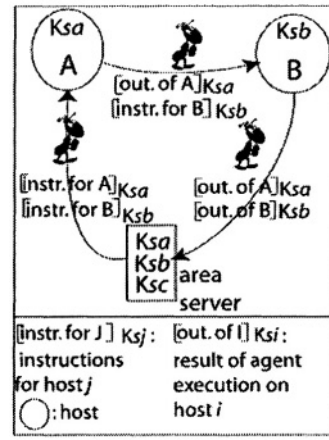

Figure 4 – Agent's secured itinerary through **a collection of hosts**

3.3. Real operation profiles construction

In order to build real operation profiles, agents are sent from the area server to the VOs infrastructure, they perform their task and they return to the area server where collected data are exploited. Parameters governing agent's activity are carefully

chosen. In fact, previous data collection or assumptions enables to orient relevant information research. Thus, the aim of a data collection session is to refine already existing profiles. Agents can work on several equipment, one after the other and can be programmed to execute everything that can be done on a computer (command execution, modifications of configuration…) and to retrieve the results. Figure 5 shows the case of simple parameter collection (CPU rate) and retrieval, but much more evolved operations can be done. Figure 6 shows a complex operation : log file parsing on several equipment (for example firewall log file) to extract relevant information (abnormal accesses), and return to the area server.

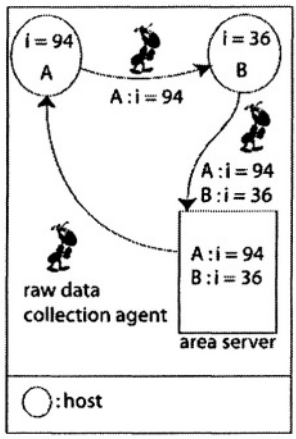

Figure 5 – Raw data collection

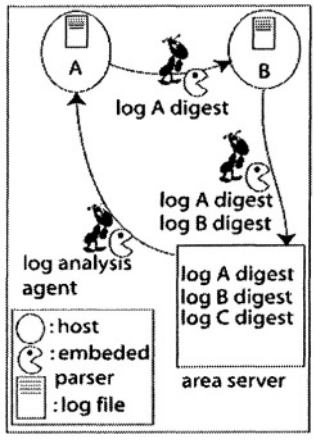

Figure 6 – log analysis

We experiment our mobile agent management platform on a simple case study which consists in 2 organisations involved in a VO (figure 7) where O1 hosts the major part of the shared information system. We aim to identify the collaboration and the real information hosting strategy (i.e. respect of the O1 hosting or the use of a replicated organisation). For this purpose, we monitor strongly the inter-organisation router and send agents to collect the traffic rate between the 2 organisations: internal agents collect O1's sub-network traffic whereas external agents are used to measure the traffic level between O1 and O2. Both of these agents collect data on a regular basis (every minutes). Data were collected between 9 and 11 AM on a regular business-day. The results presented figures 8 and 9 bring to light two different profiles:

- O1 internal traffic (figure 8) corresponds to direct accesses to database servers. The "sent" traffic is very regular because it is made of database requests. This traffic has a very low standard deviation (3699) compared to its mean (38817). The "received" traffic is very erratic and important, it corresponds to data transfers which have been requested. This erratic traffic has a very high standard deviation (118606) compared to its mean (398032).
- The traffic evolution between O1 and O2 (figure 9) show traffic bursts, one following the other twice an hour. Such a traffic profile can be related to file exchange leading to a replication process organisation: Twice an hour, O2 extract data from O1, then the processes are achieved locally (so that actors

from O2 can use their own BP instead of the shared BP...) and the updated data are sent back before beginning a new replication cycle. The "sent" traffic and the "received" traffic in this situation have almost the same mean and the same standard deviation, and the standard deviation **(≈15400000 bytes)** is much more important than the mean **(≈5500000 bytes)**. The main interest of such BP rebuilding process relies on anonymous data collection and analysis so that data privacy requirements can be fit.

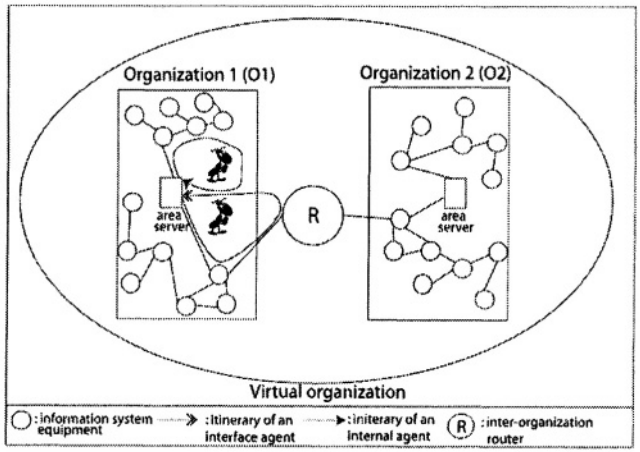

Figure 7 – an example of the mobile-agent infrastructure deployment

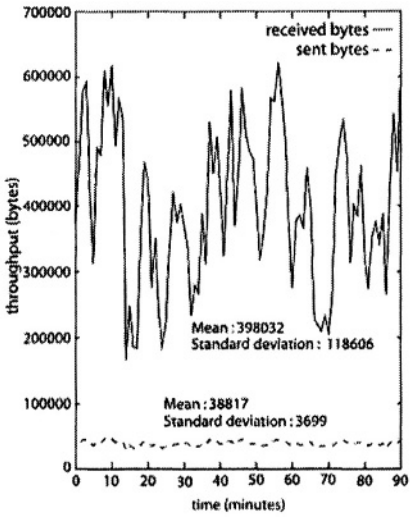

Figure 8 – internal agent results

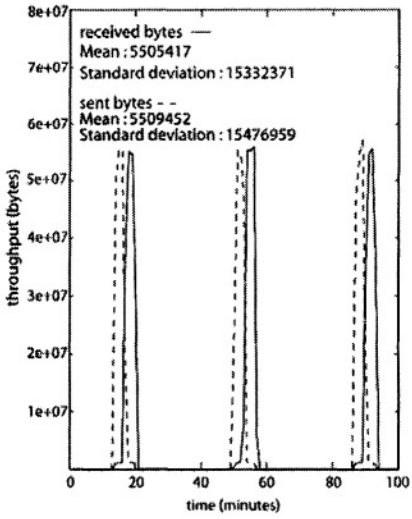

Figure 9 – external agent results

4. CONCLUSION AND FURTHER WORK

In this paper, we proposed a secured mobile agent architecture to support BP reengineering thanks to infrastructure management data. By using Business Process information, we can define behaviour profiles for the infrastructure resources and then capture the real resource use, thanks to innovative approaches such as intrusion detection concepts. Nevertheless, the data analysis process should be developed to increase the current process signature knowledge base, may be thanks to immune algorithms.

5. REFERENCES

1. Agerwala M., *"Data Flow Systems",* IEEE Computer **15** (1982), no.2,10-13.
2. Caro G.D., Dorigo M., *Antnet: Distributed stimergic control for communications network,* Journal of Artificial Intelligence Research **9** (1998), 317-365.
3. Caswell B., Beale J., Foster J.C., and Posluns J., *Snort 2.0 intrusion detection,* 2003.
4. Chou L.D., Shen K.C., and Kao C.C. Implementation of mobile-agent-based network management systems for national broadband experimental networks in Taïwan. *Lecture Notes in Computer Science.* 2744, 2004
5. Forrest S., Hofmeyr S.A., and Somayaji A., *Computer Immunology,* Communications of the ACM **40** (1997), no. 10, 88-96.
6. Garfinkel S. and Spafford G., *Practical Unix and Internet Security,* **3rd** ed., O'Reilly Associates, 2003.
7. Hammer M., Champy J., Reegineering the corporation: *A manifesto for business revolution,* HarperCollins, New York, 1993.
8. Harrison C.G., Chess D.M., and Kerschenbaum A., *Mobile Agents : Are they a good idea ?,* Tech Report, 1997.
9. Hwang S.Y. and Yang W.S., *On the discovery of process models from their instances,* Decision Support Systems **34** (2002), no. 1,41-57.
10. IETF, *RFC 1510 : The Kerberos Network Authentication Service (v5),* http://www.ietf.org/rfc/rfc 1510.txt. 1993.
11. Lange D.B. and Oshima M., *Programming and deploying java mobile agents with aglets,* Addison-Wesley, 1998.
12. Lee H. and Shepherdson J. A component based multi-agent architecture to support mobile business processes. In *Multi-Agent Systems and Applications III : 3rd International Central and Eastern European Conference on Multi-Agent Systems, CEEMAS,* Prague, Czech Republic, 2003.
13. Maruster L., Wortmann J.C., Weijters A.J.J.M, and van der Aalst W.M.P., *Discovering distributed processes in supply chains,* Collaborative systems for production management (Eindhoven, The Netherlands), IFIP Working Group 5.7. on Integrated Production Management, Faculty of Technology Management, Technische Universiteit Eindhoven, 2002.
14. Posegga J. and Karjoth G., *Mobile Agents and Telco 's Nightmares,* Annales des télé communications **55** (2000), no. 7-8, 29-41.
15. Rabelo R.J., Wangham M.S., Schmidt R., and Fraga J.S. Trust building in the creation of virtual enterprises in mobile agent-based architectures. In *4th IFIP Working Conference on Virtual Enterprises, Pro-VE'03,* Lugano, Switezerland, 2003.
16. Reuter E. and Baude F. System and network management itineraries for mobile agents. In *Mobile Agents for Telecommunication Applications : 4th International Workshop, MATA 2002,* Barcelona, Spain, 2002
17. Suh Y., Namgoong H., Yoo J., and Lee D. design of a mobile agent-based workflow management system. In *Mobile Agents for Telecommunication Applications : Third International Workshop, MATA 2001.,* Montreal, 2001.