# A Multiagent Based Approach to Money Laundering Detection and Prevention

Cláudio Alexandre and João Balsa
*LabMAg, Universidade de Lisboa, Lisboa, Portugal*

Keywords: Multiagent Systems, Intelligent Agents, Money Laundering.

Abstract: The huge amount of bank operations that occur every day makes it extremely hard for financial institutions to spot malicious money laundering related operations. Although some predefined heuristics are used they aren't restrictive enough, still leaving to much work for human analyzers. This motivates the need for intelligent systems that can help financial institutions fight money laundering in a diversity of ways, such as: intelligent filtering of bank operations, intelligent analysis of suspicious operations, learning of new detection and analysis rules. In this paper, we present a multiagent based approach to deal with the problem of money laundering by defining a multiagent system designed to help financial institutions in this task, helping them to deal with two main problems: volume and rule improvement. We define the agent architecture, and characterize the different types of agents, considering the distinct roles they play in the process.

## 1 INTRODUCTION

In the financial sector, one of the top priorities of any government is the quest for the improvement of the processes that try to prevent all illegal activities that can lead to capital loss. One of these activities, money laundering, has primordial importance since it is frequently a transnational crime that occurs in close relation to other crimes like illegal drug trading, terrorism, or arms trafficking.

Anti-money laundering (AML) regulations are typically defined by a country's monetary authority (usually a central bank) and must be complied by all financial institutions. Although corresponding to well defined rules, due to the huge amount of information that is available (namely, bank operations), and to the fact that it takes too much time for financial institutions to guaranty compliance with these AML regulations, detect and report possible money laundering activities, it is hard to track all suspicious transactions, and to deal with them in due time.

Besides, not only the proportion of money laundering related transactions is very small — about 0,05 % according to (US Congress – Office of Technology Assessment, 1995c) —, but also most occurrences of malicious behavior are a result of a set of transactions that span over a long period of time (that might be several months).

This motivates the need to develop tools that can help institutions deal with these huge amount of information, and filter what is relevant. These tools need to incorporate not only the standard regulations produced by monetary authorities, but also the expertise of human analyzers. On the other hand, it is crucial to improve the decision process (and its subjacent rules), taking into account the history that already exists on this matter, namely transactions and ultimate decisions regarding their criminal nature.

In the following sections we will start by defining the problem in more detail (section 2), and refer to some related work (section 3). Then we will present our approach (section 4), and finally present some conclusions and the plan for future work (section 5).

## 2 PROBLEM DEFINITION

Turner (Turner, 2011) characterizes money laundering as involving "the use of traditional business practices to move funds and the people that engages in this activity are doing so to make money". Traditional definitions characterize money laundering as a set of commercial or financial operations that seek to incorporate in a country's economy, in a transient or permanent way, illicitly obtained resources, goods or values. These operations develop by means of a dynamic process that typically includes three indepen-


Alexandre C. and Balsa J..
A Multiagent Based Approach to Money Laundering Detection and Prevention.
DOI: 10.5220/0005281102300235
In *Proceedings of the International Conference on Agents and Artificial Intelligence* (ICAART-2015), pages 230-235
ISBN: 978-989-758-073-4

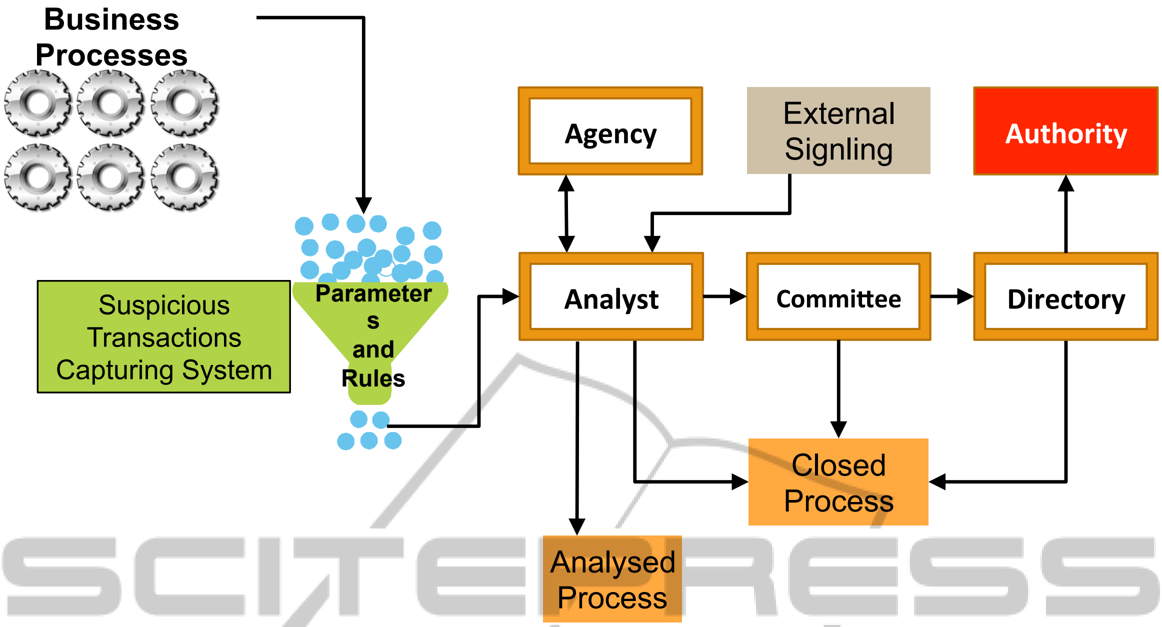


Figure 1: The whole process.



dent stages — placement, occultation (or layering), and integration — that might occur simultaneously.

*Placement* corresponds to the money introduction in the financial system, usually made through discrete bank deposits or small amount active purchases. *Occultation* corresponds to the carrying out of financial operations with the goal of dissimulate the money source. This is obtained through a diversity of transfers between bank accounts that will ultimately be concentrated in a single one. Finally, *integration*, is the incorporation of the value in the economy, for instance through goods acquisition.

So, the role of financial institutions is to find ways of spotting, in the huge amount of operations that occur everyday, the ones that might be related to a suspicious operation and then investigate them.

As we can see in figure 1, where the whole process is schematized, diverse financial business process produce huge amounts of transactions that are, in a first step, filtered, using a set of parameters and rules[1] defined in a capturing system. Some of these transactions are then analyzed by a human analyst (the *compliance analyzer*) that, considering additional external signaling information and, if needed, additional information from the bank agency, subsequently decides whether to close the process, send it immediately to a superior committee, or keep it marked for further investigation. The process might ultimately be sent to the regulatory authority or might be closed. So, the *Analyst*, the *Committee*, and the *Directory* represent three decision levels within a financial institution. Any of them can recommend the process to be closed or send it upwards.

Of course, the Central Authority receives information from many institutions and must have a way to process them and produce their own final decisions, sometimes providing their own feedback to individual institutions. But our focus here is in the process inside one institution, and on how to improve and make more efficient the decision processes involved.

## 3 RELATED WORK

Regarding the analysis of bank transactions, according to (US Congress – Office of Technology Assessment, 1995c), there are four categories of technologies that are useful and that can be classified by the task they are designed to accomplish: wire transfer screening, knowledge acquisition, knowledge sharing, and data transformation. These technologies form the basis of the definition of a set of policy options that can be adopted in order to fight money laundering (US Congress – Office of Technology Assessment, 1995a). These options include, among others, the definition on an *automated informant*, an AI based system to monitor transfers, and a computer-assisted examination of wire transfer records by bank regulators.

[1]These parameters and rules are typically based on a mapping from the regulations imposed by the country's monetary authority, usually a central bank.

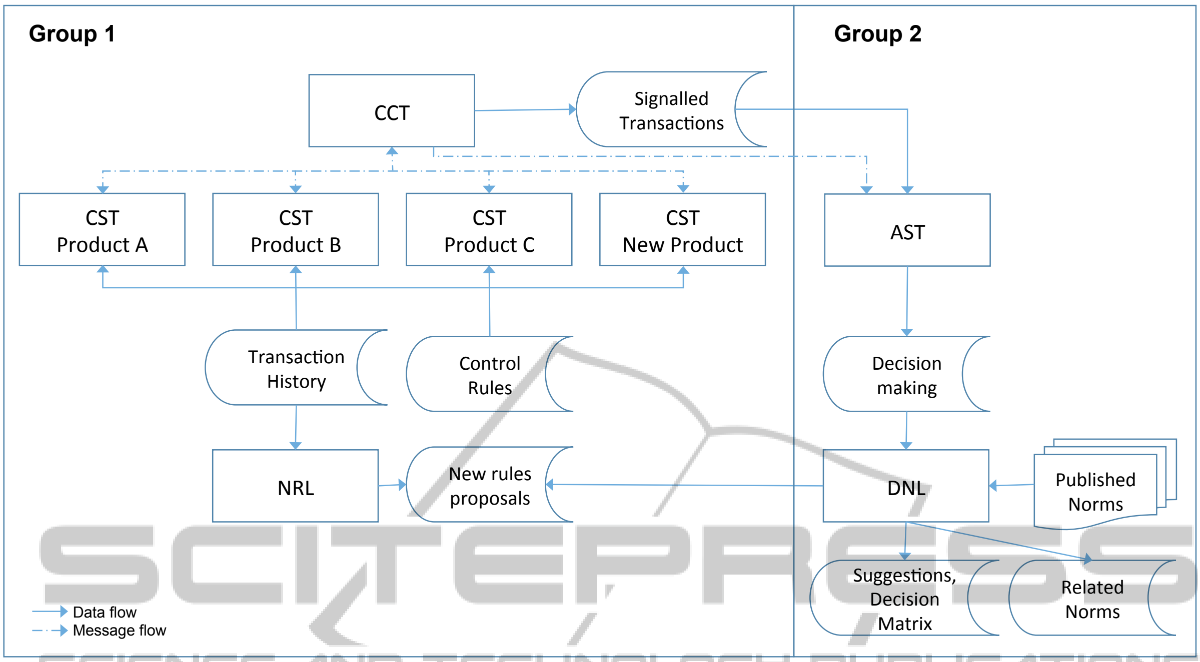




Figure 2: Agent Architecture.

Regarding the use of agent based approaches in AML, there are very few authors that have considered them. In (Gao et al., 2006), an agent architecture is defined to include a set of specialized agents, such as data collecting agents, monitoring agents, a behavior diagnosis agent, and a reporting agent. This last agent is responsible for issuing alerts regarding potential money laundering operations.

Another approach (Gao and Xu, 2010) is supported in the definition of a Real-Time Exception Management Decision Model that is used to inform a multiagent based real-time decision support system to detect money laundering operations. These authors design their system defining three groups of agents: the *Intelligence* group, with agents responsible for collecting data, profiling clients, and monitoring transactions; the *Design* group, where the critical analysis are made; and the choice group, responsible for reporting and user interface.

Another agent-based approach is the one presented in (Xuan and Pengzhu, 2007). Besides the inclusion of reporting and user agents, much alike what is done in the above mentioned works, these authors include Negotiation and Diagnosing agents that ultimately are responsible for the most critical decisions, taken on the basis of information provided by two other groups of agents: data collecting and supervising.

In (Kingdon, 2004), it is proposed that an artificial intelligence approach should model individual clients and look for unusual rather than suspicious behavior.

There are also statistical approaches, like the ones described in (Liu and Zhang, 2010) and (Tang and Yin, 2005), but we won't go here into details regarding this type of approaches.

## 4 AN AGENT-BASED APPROACH

The motivation for using an intelligent agent based approach departs from the analysis of the problem (figure 1), and from the observation that some of the tasks that we want to automatize (at least partially) match perfectly the principles behind multiagent system definition (Wooldridge, 2009). We need a set of entities (agents) with autonomy to perform specific tasks and to engage in communication with others in order to accomplish a certain set of goals. Each agent has its own knowledge and must be able to reason and decide in an intelligent manner. Besides, we aim at flexibility and scalability which is obtained with the architecture we propose. Agents also provide a more natural way to model and program features like communication, reasoning and decision making (Demazeau, 1995).

We consider two groups of agents, according to their role in the process. The first corresponds mainly to a group of agents responsible for the *capture* of suspicious transactions (CST), whilst the second corresponds to the agents that perform the *analysis* of sus-

Table 1: Agent Characterization.

| Agent | Input | Internal Processes | Actions | Properties |
|---|---|---|---|---|
| CST | Set of transactions in a time interval | Transaction-oriented analysis. Signal transactions. Client-oriented analysis. | Communicate signaled transactions. Communicate suspicious clients. | Reliability Precision |
| CCT | Signaling message from CST agent | Manage communication with CST agents. Storage signaled transactions. | Communicate suspicious clients. | Agility |
| NRL | Transaction history | Data mining on existing transactions. | Suggest new parameters and rules. | Adaptability |
| AST | Suspicious transactions | Analyse signaled transactions. Simulate compliance officer. Decide subsequent procedure. | Communicate decision. | Reliability Autonomy Precision |
| DNL | Decision history. Published norms and regulations. | Learning based on compliance officer decision history. Infer new capture parameters. Propose new decision procedures. Recognize relevant norms. | Suggest new rules and parameters. Suggest novel decision procedures. | Precision |



picious transactions (AST) signaled by the agents of the first group.

In figure 2 we present a schematic view of the global agent architecture and system flow.

## 4.1 CST Agents

As previously mentioned (recall figure 1), data is originated in several business processes. We define an agent for each product (current accounts, investment funds, currency exchanges, ...). This approach has two advantages. Firstly, this allows us to model each agent's knowledge according to the specificities each product has. Secondly, it makes scalability easier, in the sense that the creation of a new product can be incorporated in the system just by adding a new agent specialized in it.

Besides these specialized agents, there is one that is responsible for the communication of captured transactions (CCT), as well as its storage for further use.

Whenever a CST agent identifies a suspicious transaction, it sends it to CCT that is responsible for forwarding it to some other CST agents. So, CST agents have two working modes:

**transaction oriented** In which agents try to capture suspicious transactions with no assumptions regarding clients.

**client oriented** In which agents try to capture suspicious transactions for clients that were signaled by other CST agents.

Finally, this group has a third type of agents — New Rule Learning (NRL) — that are responsible for learning new capturing rules regarding each product.

## 4.2 AST Agents

These agents perform the analysis of the previously signaled transactions. Agents of these group have autonomy to decide amongst three possibilities regarding a signalization: accept it, discard it, or send it for further (human) analysis.

So, these agents assume the role of compliance officers in the analysis of suspicious transactions. They have a learning component that contributes to the improvement of the control parameters and to the enlargement of the set of situations that can be decided automatically.

Also in this group, there is the decision and norms learning agent (DNL). This agent is responsible for the improvement of the decision matrix. Taking into account all decisions made (namely, those produced by human experts), it is responsible for finding possible refinements or new inclusions in the base parameters. Additionally, in a different dimension, this agent processes new regulations in order to find new norms that need to be implemented.

### 4.3 Agent Properties

In table 1 we summarize these agents' main inputs, their main internal processes, their actions, and some desired properties. We characterize each type of agents in terms of what are its inputs, its main internal processes, the actions they can perform, and some agent related properties.

### 4.4 Agent Interaction

Cooperation among CST agents happens through their direct interaction with the CCT agent, that coordinates the tasks and receives the results. Interaction amongst other agents (CCT, AST, DNL, NRL) has the role to trigger in each of these agents the goal to perform the task under its responsibility. In other words, all agents have their own specific expertise, and they have independent and not conflicting goals. So, in this model there isn't the conflicting goals problem or the need for negotiation among agents. On the other hand, there is plenty of cooperation for the achievement of a common goal.

CST and AST agents learn and evolve to reduce the false positive problem, common to systems based only on a set of rules and patterns of behavior (Gao et al., 2006; Le Khac and Kechadi, 2010).

## 5 CONCLUSIONS

The main goal of this contribution is to present a novel approach to money laundering detection and prevention. This is an ongoing research that has the ultimate goal of contributing to AML process improvement in a concrete organization.

It is consensual that the task is hard and far from being solved, which establishes the relevance of this work.

As mentioned in section 3, other authors have explored agent-based approaches to this problem. Nevertheless, our work is distinguished from those, for start, in the architecture we defined, namely on the explicit integration of learning components, and in the inclusion of product specific agents.

There are two main paths in this project. One relates to the definition and implementation of the multiagent system that will be the basis of the new decision making process. The other relates to the learning of new rules and parameters that will serve as valuable resources for the agents defined. This second part relies heavily on real data concerning transactions in financial institutions.

There is a lot of work still to be done in both paths. We present the most relevant for now in the following section.

### 5.1 Future Work

Regarding agent models, they still need to be refined. Regarding CST agents, the first product to be included is the "current accounts", which is currently being done. Then we will proceed to other products.

In another trend, we are also working on behavior modeling (recall that suspicious behavior cannot be found by looking at isolated operations). We are building behavior patterns that consider large time spans. This will allow the decision process of the CCT agent.

Regarding NRL agents, apart from the identification of product specific properties/rules, we're trying to find cross-product relations, that is, finding, for each client, in what way are suspicious transactions regarding a product related to transaction patterns in the other products. The ultimate goal is to obtain new parameters to be used by CTS agents.

## REFERENCES

Demazeau, Y. (1995). From interactions to collective behaviour in agent-based systems. In *Proceedings of the 1st. European Conference on Cognitive Science. Saint-Malo*, pages 117–132.

Gao, S. and Xu, D. (2010). Real-time exception management decision model (RTEMDM): Applications in intelligent agent-assisted decision support in logistics and anti-money laundering domains. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, pages 1–10.

Gao, S., Xu, D., Wang, H., and Wang, Y. (2006). Intelligent anti-money laundering system. In *Service Operations and Logistics, and Informatics, 2006. SOLI '06. IEEE International Conference on*, pages 851–856.

Kingdon, J. (2004). AI fights money laundering. *Intelligent Systems, IEEE*, 19(3):87–89.

Le Khac, N. A. and Kechadi, M.-T. (2010). Application of data mining for anti-money laundering detection: A case study. In *Proceedings of the 2010 IEEE International Conference on Data Mining Workshops*, ICDMW '10, pages 577–584, Washington, DC, USA. IEEE Computer Society.

Liu, X. and Zhang, P. (2010). A scan statistics based suspicious transactions detection model for anti-money laundering (aml) in financial institutions. In *Multimedia Communications (Mediacom), 2010 International Conference on*, pages 210–213.

Tang, J. and Yin, J. (2005). Developing an intelligent data discriminating system of anti-money laundering based on svm. In *Machine Learning and Cybernetics,* *2005. Proceedings of 2005 International Conference on*, volume 6, pages 3453–3457 Vol. 6.

Turner, J. E. (2011). *Money Laundering Prevention: Deterring, Detecting, and Resolving Financial Fraud*. Wiley.

US Congress – Office of Technology Assessment (1995a). Conclusions and policy options. In (US Congress – Office of Technology Assessment, 1995b), chapter 7, pages 119–144.

US Congress – Office of Technology Assessment (1995b). *Information Technologies for Control of Money Laundering*. US Government Printing Office.

US Congress – Office of Technology Assessment (1995c). Technologies for detecting money laundering. In (US Congress – Office of Technology Assessment, 1995b), chapter 4, pages 51–74.

Wooldridge, M. (2009). *An introduction to multiagent systems*. John Wiley & Sons.

Xuan, L. and Pengzhu, Z. (2007). An agent based anti-money laundering system architecture for financial supervision. In *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on*, pages 5472–5475.