Towards a General Definition Of Trust and its Application to Openness in MAS

PhD student paper

G. Muller
muller@emse.fr

L. Vercouter
vercoute@emse.fr

O. Boissier
boissier@emse.fr

Dpt SMA/SIMMO, ENS of Mines of Saint-Etienne
158, Cours Fauriel, 42023 Saint-Etienne, France

ABSTRACT

Trust-based systems help entities integrating risk of defection in their interactions with others when their benevolence and trustfulness can not be guaranteed.

The study of various works from different fields of research, helps us extracting a few common points to determine what concepts trust is based on. Then, we build a formal definition of trust, reputation and confidence concepts and related processes.

To formalize the definitions, we propose a framework based on the actors of trust-related processes. This framework seems general enough to include works from social sciences and e-commerce. We, then, focus on the problem of management of openness in a decentralized multi-agent system and present a solution based on trust as formally defined in our framework.

Introduction

The spread of computers and networks makes people interactions easier. It is obvious that, if the outcome of an interaction is crucial for one of the parties involved, this one would need a way to reduce uncertainty of the behavior of the other. Security-based systems are used to reduce the uncertainty of exchanged messages and the identity of the sender and the receiver, but it does not prevent the other party from lying (forging the *content* of information). In human societies, the adopted solution, to reduce risks, is to use trust-based systems. It is a sufficiently generic solution, so it appears that, even if some parameters have to be gauged according to the application, the great principles might be valid in artificial societies.

In fact, the study and modeling of trust-based systems, involves more and more researchers from various domains. It is really a complex concept and no consensus has yet been found to define it. Trust was first studied as a specific topic in 1979 ([8]). More recently, different researches have been done in social sciences ([18, 13, 1, 3]), in e-commerce ([6, 5]) and in multi-agent systems ([10]) in order to try to build a general theory of trust and to distinguish this concept from others such as sincerity, honesty, confidence, reputation, security, dependability, quality, dependence, uncertainty, risk, cooperation, delegation, norms, bet, representation of the others...

Moreover, some research has been done to compare different points of view about trust in various disciplines ([2, 5, 10, 9]).

Based on a very large panel of definitions gathered from various domains and various reviews in specific fields of research or overlapping several, section 1 extracts common points of these definitions.

Given this basic set of concepts trust is based on or related to, we will build (section 2) a general framework by distinguishing the different actors in several situations, leading to a first step in defining formally trust, reputations, confidence and their processes.

Then, we briefly present the problem of openness in decentralized mutli-agent systems, together with a solution based on the previous definitions of trust-related concepts.

Although, the aim of this formalization was to have a framework for the solution of the openness problem, it seems generic enough to allow to model other concepts as found in social sciences and in e-commerce. Two examples from these domains are thus modeled within our framework ([3] and [16]).

1. GLOBAL OVERVIEW OF TRUST

The main difficulty when working on trust is that there is no precise and acknowledged definition of the concept, this section aims at giving a global overview of the literature.

1.1 Lots of Definitions

There is lots of definitions of the concept of trust (see for example p. 35 [2] quoting SHAPIRO "confusing potpourri"). Each author has his own definition, often mixing different concepts such as risks, uncertainty, quality, competence, reliability, dependence, honesty, sincerity, security, etc. Various reviews (e.g. [2, 5, 10, 9]) have been made, to distinguish between those concepts, but there is still no commonly ac-

AAMAS '03 Melbourne, Australia

knowledged definition.

QUÉRÉ ([12]) establishes an important distinction between the *mental state of trust* (being trusty, to have trust in someone) and the *act of trusting* (to act with/towards someone due to trust one has in him). CASTELFRANCHI and PEDONE ([2]) add a middle step: *intention of trust*. When the level of trust in the current *mental state* of an agent is sufficient, then the agent may have the *intention* to trust, but, for some external reason (physical, emotional,...) the agent may not *act*. In this paper we focus on trust as a mental state, since it is the source of the intention to trust and of a trusty-behavior; it implies trust as an action process. Moreover, as stated in [2], trust as a behavior is difficult to distinguish from cooperation.

However, some general ideas are common in those various definitions. First, the representation as a belief (that, thus, could be false) that is leveled (**A** can trust **B** more than **C**). Second, since the evaluation could be false, there should be some processes to re-evaluate the level value regularly or when its falseness is established. Finally, the social components of trust (in [1], an agent **X** can only trust an agent **Y** for $\mathbf{g}/\alpha$, where **g** is a goal and α is the action **X** wants **Y** to do, in a general delegation framework).

1.2 Different Kinds of Trusts

Previous section showed the common points of various definition and that trust should be a personal attribute, built by an agent for himself. However, this remark is in contradiction with the social dimension of trust. It would then be interesting to establish a distinction between the trust built by an agent on its own and trust built with the help of others.

In the latter case, we also have to classify all the ways an agent have to be helped building its trust:

First, the *source* of the information may not be without importance: either the information came from an anonymous source, or for an identified one. In the latter cas, the social relationships between agents (friendliness, hate, cooperation, competition,...) influences trust relations: for example, if the agent **X** that gave **Y** its trust in **Z** is close to **Z**, it should tend to be more lenient that if it didn't know **Z**. If **X** knows **Y** it will tend to be more accurate in the information it gives about **Z**.

Second, the *content of the transmitted information* may already be an evaluation of the trust one has in another, or it may simply be a raw information, without any interpretation from the sender.

Thus, previous distinctions upon the source and the content of the "message" (not restricted to the computer view) of trust, which is passed on from agents to agents, implies a distinction through different notions of "trust", that will probably have to be labeled another way.

Finally, one may also discern another case. Indeed, when an agent has neither a local perception of what trust it may have in another one, nor can be helped by others, what should it do? Maybe it should call upon hard-coded values or rules, implying the existence of norms and/or of some kind of institution.

It should be obvious from now that trust is a complex concept. Very few of the models studied distinguishes all the emphasized notions presented above. Moreover, trust and reputation are often viewed as a single concept, when we argue, following CASTELFRANCHI and FALCONE ([1]), and SABATER and SIERRA [16], that it is a multi-dimensional concept.

2. MODELING TRUST

We argue, following CASTELFRANCHI and PEDONE ([2]) that trust may apply, not only to a single agent, to groups of various sizes, and that do not enter in consideration in defining the concept.

Since trust is viewed as a social concept, its benefits should not be limited to the individual. Considering the target as a person would be reducing the considerations to a small set of cases, where one can ascribe intentions, motivations, interests, reason and goals to the target. Since "agents" are the smallest units to refer to individuals, groups, organizations, communauties and institutions, we will prefer this term when refering to trust-related concepts.

In some cases, trust applies to an object, or something without intention, motivation, interest, reason or goal. Thus, in those cases the target, for example, might be an object. The object can not, in a multi-agent sense, play the role of "Target", thus it is a role ascribed to the object by the Beneficiary or the Observers. That is not the focus of this paper, but it should probably be analyzed carefully (problem of "reciprocity", in [3, 10, 11]).

2.1 General Framework

The first role to consider is the **Target** of the evaluation. Some attribute α of the agent playing this role is (if possible) *being observed* by some **Observers** in its interactions with other agents (right part of figure 1).

The role "**Beneficiary**" defines the *final recipient* of the trust evaluation of the Target for its attribute/ability α.

Three other roles may be distinguished as intermediaries in the processes (see 2.3 for the complete description of two processes) of building trust.

Agents that play the role of **Observers** observe other agents interacting and accumulate *raw data* about their interactions. **Observers** are able to communicate these data to some agents that can exploit and analyze them. Such agents are called "**Evaluators**". The **Evaluators** can use raw information from **Observers** or aggregated data from other **Evaluators** in order to merge them. An *evaluation function* is used to merge some *inputs*, which number and type depends on the attribute being evaluated (α).

The role of **Gossipers** is to transmit information of trust or related concepts to the beneficiary.

2.2 Definitions

2.2.1 Trust Relation

Trust is the *belief* in someone else's actions acquired by *direct experiences*.

Since it is a belief, it can be false. Moreover, one can reason on this belief, making it possible to perform iterative reasoning : since **X** knows that **Y** trusts him, what does it imply if **X** performs action a?

Since it is acquired by direct experiences, it is a property of the owner and no one can interfere with that. It allows different agents who have had different experiences to have different trust levels regarding the same target agent. In the same way, it allows an agent to change his mind over time.

Trust is a property of an agent, owned by this agent, based on direct experiences. Trust is thus defined when no agent

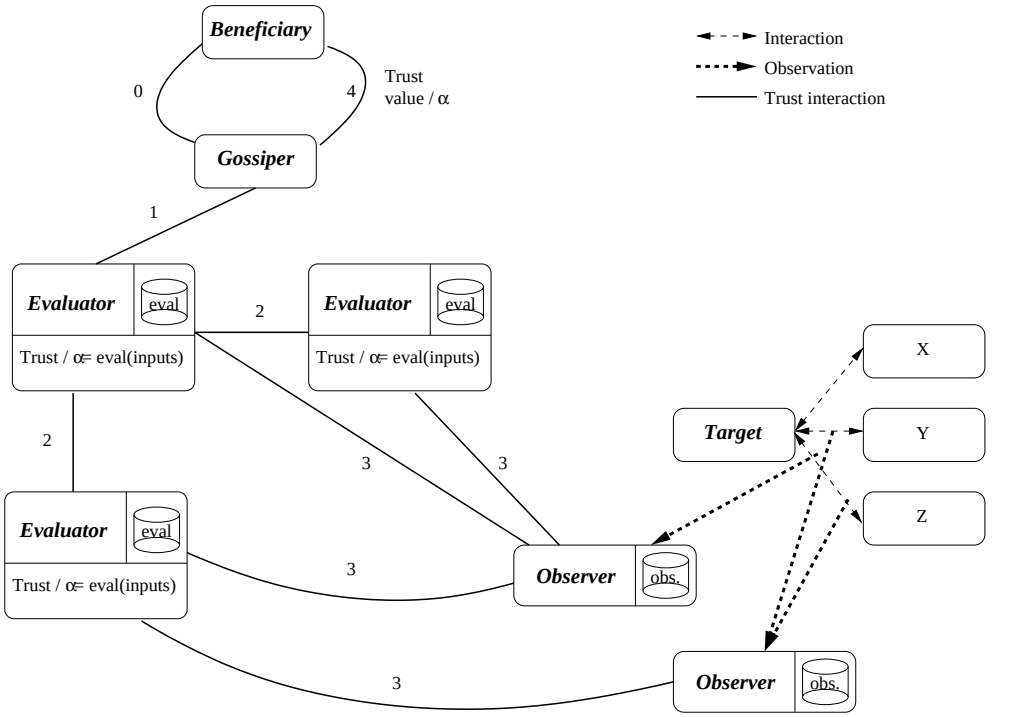

Figure 1: Interactions between the roles.

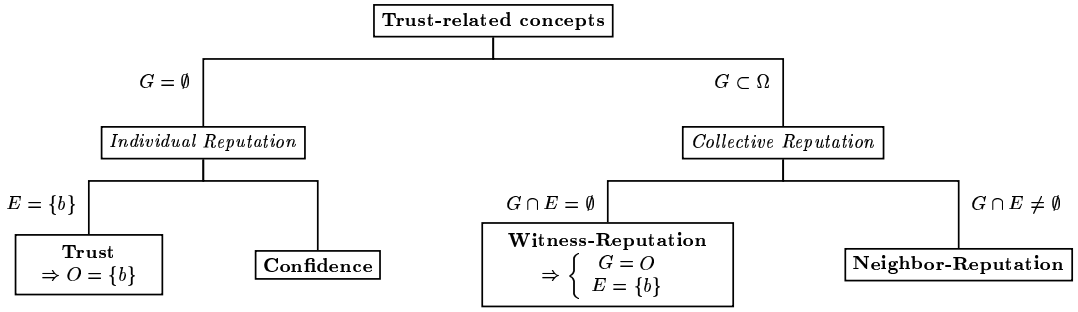

Figure 2: Organization of trust-related concepts.

plays the Gossiper role and when the agent that plays the Beneficiary role also plays the Observer and the Evaluator roles.

Figure 2 shows the relation between the roles for one instance of one of the two trust construction processes (described section 2.3), from the point of view of one Beneficiary. Ω is the set of all the agents.

2.2.2 Reputation Relations

Reputation is commonly viewed as *the image a group has of an individual.* A Reputation is a *belief* (that could be false) in an ability of another agent, acquired not only by direct experiences, but maybe with the help of other agents too.

Since reputation is built with gossip (gossip can be positive, it is not restricted to calumny) it is closely related to the diffusion of trust-related notions which are described section 2.3.

Since reputation is built through observations by a group of agents (maybe including the Beneficiary himself), it differs from trust by the number of Observers and Evaluators. Thus, trust is a restriction of reputation and could then be defined as an "Individual Reputation" [16], where the groups of Observers and Evaluators are limited to the agent itself.

So far as reputation is concerned, the sender of the information can belong to one (or more) of the two subsets of agents:

Neighbors Subset of acquaintances at a given time;

Witnesses Neighbors who have observed *direct interactions* of target.

The **Witness-Reputation** will be defined as the reputation built upon information gathered from Witnesses, while **Neighbor-Reputation** will represent information gathered from Neighbors (right part of the figure 2). Intuitively, but not necessarily, Witness-Reputation should be more accurate than Neighbor-Reputation. Other kinds of Collective-Reputations are probably possible to define.

2.2.3 Confidence Relation

Confidence can be viewed as trust in institutions ([8]) or in marks ([18]). It is not updated everyday. Confidence in the Target "t" for the attribute α can be built upon values admitted to be true by all the agents (or a great majority), thus modeling an institutional law. It can be represented by a hard-coded value put in the system by its designer. The confidence is established through some kind of shared view of the system and due to the absence of Gossiper.

Figure 2 shows the links between Trust, Reputations and Confidence from the Beneficiary point of view.

It is obvious that we define a small set of concepts regarding to the possibilities offered by the framework (section 2.1).

If $\mathcal{O}$ is the set of agents playing the role of Observers, $\mathcal{E}$ the set for the Evaluators, $\mathcal{B}$ the Beneficiaries, $\mathcal{G}$ the Gossipers... We can distinguish other concepts through the *size* of $\mathcal{O}$, $\mathcal{E}$, $\mathcal{B}$, $\mathcal{G}$... (0, 1, several agents...). For example, we can say trust and reputation differs with regard to the number of agents in $\mathcal{E}$ or $\mathcal{O}$, or *the overlapping* of the different sets; we distinguished Witness-Reputation from Neighbor-Reputation with the help of the sets $\mathcal{G}$ and $\mathcal{E}$ (figure 2).

CONTE and PAOLUCCI ([3]) try to characterize the "quality" of the reputation through this kind of overlapping in terms of under/over-rating and under/over-evaluation (under-rating means few people give ratings about the Target, while under-evaluation means the accuracy of the final evaluation).

2.3 Trust Construction

Now that all the roles have been presented, focus will be on the *processes* involved in trust establishment. Two processes can be distinguished. The first one starts from the Beneficiary, the second from the Observers.

If, for some reason (e.g. in an E-commerce application, if an agent looks for a business partner) a Beneficiary needs an evaluation of reputation about the Target for α, it may ask for this evaluation to Gossipers (link labeled 0 in figure 1) it believes to have the capability in this context. If the Gossiper is not part of the Evaluators and has no local evaluation available, it should ask an Evaluator to compute the value (link labeled 1). The Evaluator, which needs informations on the Target, can get raw observations from Observers or pre-computed values from other Evaluators (links labeled 2 and 3 in figure 1).

The other way the process can take place, is, for example, by starting with the observation of a cheat by one or more Observers (right part of the figure 1). Agents playing this role, probably will communicate the information to the Evaluators they are related to (link 3), which may, on the fly, update their trust in the Target and pass the information on the Gossiper (link 1), which, in turn, may also update, and send the information to the Beneficiaries (link 4).

These two processes involve the transmission of the information, but the information is not always of the same kind and does not always concern the same agents. There are different types of message defining the process of gossiping (not restricted to calumny [3]).

As the information comes from others, it could come from a trust evaluation (if the other have observed direct experiences of the target) or from a reputation one (if it always is aggregated informations coming from different sources). A **recommendation** is a transmitted notion of trust or reputation. There are different kinds of recommendation: if the information is a trust information or a reputation information.

A recommendation of trust is a message containing trust passed from the agent "g" (playing the roles of the Observer, Evaluator and Gossiper) to the agent "b" (the Beneficiary). Since "b" did not observed the direct experiences, it can not use the information to build its trust. It aggregates different trust recommendations to build (or modify) its Witness-Reputation (section 2.2.2, [14, 16], "Direct-Reputation" in [10]) about the attribute α of the Target "t".

A recommendation of reputation is a message containing reputation information from the agent "g" to the agent "b". This reputation has already been aggregated by Evaluators upon raw observations made by Observers and upon other aggregated evaluations. Since "b" did not observed the direct experiences, it can not use the information to build its trust. It can neither use it to build its Witness-Reputation since "g" is not the only Evalutor of the information it passes on. It aggregates these recommendations to build (or modify) is Neighbor-Reputation (defined section 2.2.2, Indirect-Reputation [10]) about the attribute α of the Target "t".

2.4 Reasoning on Trust

To compute trust-related notions, there is a need of to choose a data structure compliant with the model above.

Since there are different levels of trust (an agent can trust another *more* than a third one for the same thing), we need a set of values. In the same way, an agent can distrust a constant cheater *more* than an occasional one, so the set should include distinct positive and negative values.

The sets [-1,0[and]0,+1] seems useful as they are continuous, expressing an infinite number of values, and allowing the use of more simple mathematical equations for initializing, updating or using the value.

To represent the fact that an agent has no direct experience with the Target, the "unknown" value can be used. Then, and only then, it is possible to add the '0' value which means: "I had direct experience(s) with the Target, but I am unable to determine if I can trust it or not".

The representation is then computed in [-1,1] $\cup$ "unknown", and, first, allows to distinguish between the "unknown state" and the "neutral state" (even in the presently more complete E-commercial model [14, 16] this distinction is not established); second between the "neutral state" and the "negative states" (this distinction seems really important but is not made in Game Theoretical Models, where [0,+1] values are used).

Figure 3 shows how we use this special value "unknown" and how the different relations (Trust, Witness-Reputation, Neighbor-Reputation and Confidence) are used by each agent. The importance of the particular "unknown" value will be underlined in the scenario presented in section 3.2. The relevance of the trust value depends on the number of ratings and should probably depend on their deviation ([15]) too.

3. TRUSTY OPEN MULTI-AGENT SYSTEMS

Trust is often used to evaluate the honesty of an agent when it commits to perform a given task. But its use can be extended to most of the interactions between agents in order to estimate if an agent believes the content of a message that it sent. We are mainly interested in the exchange of informations for openness purpose when agents send some

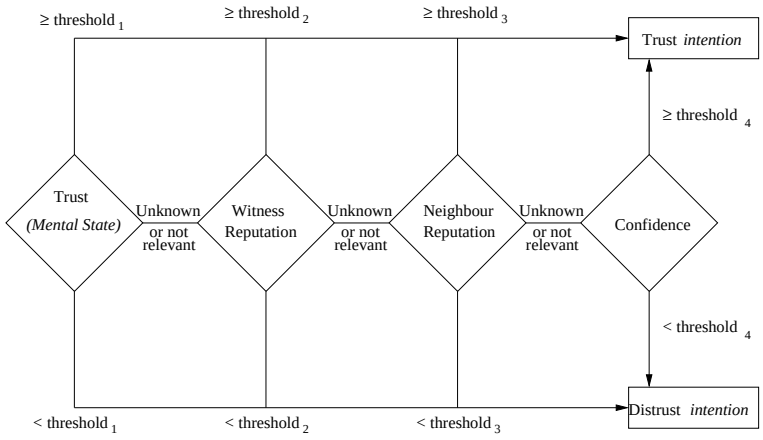

Figure 3: Current view of how to apply the model.

informations about themselves or about other agents. In this section, we show how our framework can be used to model trust evaluation in the management of the openness of a MAS.

3.1 Distributed Openness Management

In previous work [19], we proposed a distributed approach to handle the openness of a MAS which does not rely on a central entity such as a middle-agent. This work is based on the assumption that each agent has a set of **capabilities** and a set of **requirements**. Capabilities represent what an agent can do and requirements target some categories of capabilities for which the agent may seek in the future some other agent that can perform them. As the system does not have any central repository for external descriptions of the agents, each agent should keep a local representation of others that should only include relevant informations about other agents. An information is considered relevant if it is a capability or a requirement of another agent that matches one of the agent's own capabilities or requirements.

When a new agent is added to the MAS, it needs to build its own representation of others and to update the local representation of some other agents. This is done by the following process:

1. The new agent **A** follows a presentation protocol with an agent **B** of the MAS. They exchange their own external descriptions in order to build a relevant representation of each other;
2. Agent **B** compares its list of acquaintances with **A** and advices to **A** some of its acquaintances that are relevant for it;
3. **A** uses this advice to start another presentation with another agent (back to step 1).

To avoid agent **A** to present itself to every other agent, we introduced the criterion of integration that defines the amount of knowledge that an agent needs about other agents. For example, agent **A** may need to know **every** other agent that has a capability or a requirement that is relevant for it. Thus, as agent **B** is integrated to the MAS, it can act as a middle-agent for some capabilities (or requirements) because **B** knows that it knows every other agent relevant for these capabilities (or requirements). In its advices, **B** can specify to **A** that its list of acquaintances, relevant for a given capability (or requirement) is complete. Then, **A** will consider itself as integrated (and stop the iteration of presentations/advices) when it will have received complete lists of agents for each of its capabilities and requirements. More details about this work can be found in [19].

Figure 4 shows an example of this process.

In this example, an agent **A**, with a requirement x and a capability y is introduced in the MAS by the agent **B**. After a presentation of each other, **B** send advices to **A** about the agent C for its requirement on x. **B** can specify that C is the only agent of the MAS with this capability because **B** is integrated and has also a requirement on x. Then, the agent **A** will present itself to C, receive advices from C, and continue this process until it receives a full advice for its capability y.

3.2 Introducing Trust in the Openness Management

One of the assumptions of this previous work was that the agents are sincere in their presentations and advices. We illustrate here how our framework for trust evaluation can be used to drop this assumption. Let's consider the case where the agent C lied in its advices in order to hide some other agents that have the capability x. When **B** presented itself to C, agent C told it that it is the only agent that can do x. Then, agent **B** did not look for other agents that can do x and propagated this lie in its own advice to the agent **A**.

The following scenario (figure 5) illustrates how trust-related notions can be used to detect the lie and recover from it. We also show how the framework presented in section 2.1 can be used to describe this scenario.

Let's consider an agent **D**, having a requirement about x and y, which is being added to the MAS. This agent already knows (from a previous presentation) another agent **E**, with the capability x and is currently presenting itself to agent **A**. At the end of their presentation, **A** advises **D** to contact agent **C** because **C** has the capability x.

Following this advice, **D** starts a presentation with **C**. Then, as **C** continues to claim that it is the only agent that has the capability x, **D** can detect the lie because it also knows the existence of another agent (**E**) that can do x.

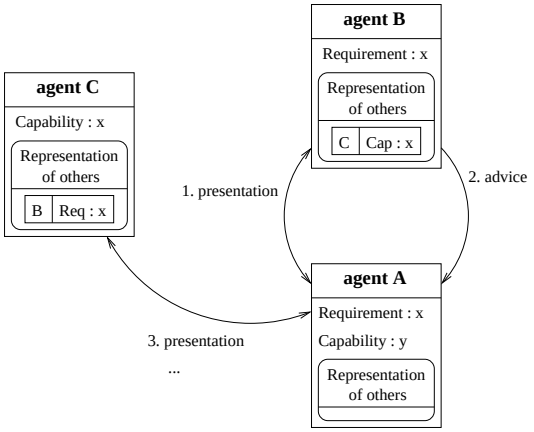

Figure 4: Example of the presentation process.

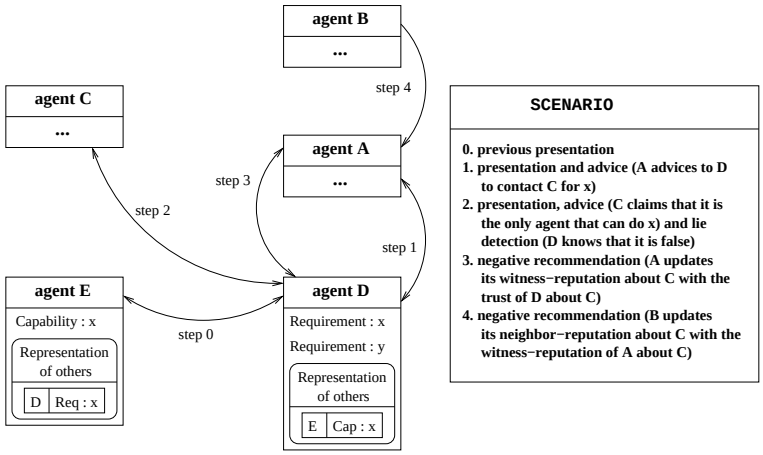

Figure 5: Using the trust framework.

After this detection, **D** updates its trust about **C** from the "unknown" value to a negative value and does not believe the advice. Agent **D** also propagates this information to the agents it knows: **A** and **E**.

We will now focus on agent **A**. At first, **A** only had "unknown" values for its trust, witness-reputation and neighbor-reputation about **C**. By default, it trusted **C**'s advice. After the recommendation from **D**, its witness-reputation for **C** was set to a negative value. That implies that the agent **A** does not believe anymore **C**'s advice and starts again other presentations to know all the agents with the capability x. **A** will also forward its witness-reputation to **B** that uses this information to update its own neighbor-reputation about **C**. Then, agent **B** will behave the same way than agent **A** did.

In this scenario, we can see how trust, witness-reputation and neighbor-reputation are used and updated. Table 1 shows the mapping between agents and roles according to the different points of view.

Some researchers ([5, 17, 20]) emphase the utility of an "unknown" value but also the difficulty to interpret this value in a decision function. In the reasoning processes that we described in the figure 3, we suggest to use this value in order to choose which trust notion (Trust, Witness-Reputation, Neighbor-Reputation or Confidence) should be taken as a numeric input of the decision function. The relevance of this reasoning process is shown in the previous scenario:

If the agents **D** and **E** had been initialized with a "neutral" reputation, like in some systems ([21, 16, 4]) with a '0' value, they would not have had enough trust in **C** to enter the system. Generalizing this case when there are few agents to introduce to, no agent would enter the system, so the system would not be an open one, which is critical in our case. It is then an obligation to distinguish between a neutral value representing Trust, Reputation or Confidence and the absence of knowledge (or low reliability of the level value) about interaction with the Target. This remark re-enforces the computer representation of trust-related concepts proposed in section 2.4.

4. RELATED WORKS

4.1 In E-Commerce

The Social Regret model ([16]) presented by Sabater and Sierra at the EASSS'03 in Barcelona about reputation in e-market places is more complete and totally compliant with the model previously presented. It is the most developed model from now on and relies on social sciences works. Moreover, it has several common features with the model we

Point of View (Beneficiary)	Evaluator	Target	Gossiper	Observer	Attribute
A	D	C	D	D	$WR_p(C,\alpha)$
E	D	C	D	D	$WR_p(C,\alpha)$
B	D	C	A	D	$NR_p(C,\alpha)$
D	D	C	(D)	D	$Trust(C,\alpha)$

Table 1: The scenario represented with the model. Where α is the ability to send advices in the openness recommendation process and the "inputs" come from the history of introducing interactions.

envisage to use in the context of the openness problem. SOCIAL REGRET uses different kinds of reputations. The first one is called "Individual Reputation". It is labelled "individual" because it uses the past experiences from the "source" agent (our beneficiary). So, since the agent uses its own experiences (observations) and evaluates the target itself, the "Individual Reputation" can be mapped to our Trust. The second kind of reputation (called "Witness Reputation") is a more social one (from which the "Social" Regret system draws its name). It consists in aggregating informations from Witnesses (agents "close" to the source). The authors then consider using the social relations between the agents to determine which agents can be Witnesses. This kind of reputation is the same as our own Witness-Reputation and formalize the same way within the Observator, Evaluator, Target, Beneficiary and Gossiper roles. The third sort of reputation is called "Neighbourhood Reputation", but diverge consequently from our Neighbour-Reputation. Indeed, their Neighbourhood-Reputation uses relations of the target, when our Neighbour-Reputation uses relations of the beneficiary. The Neighbourhood-Reputation is computed by an estimation of the behaviour the target may have through observation of the behaviour of agents socially close to it (see [4, 3] for the same idea of classifying agents following their interest). This sort of reputation will not be used in our model since we may not be able to classify agents. However, that do not prevent our general framework to represent this kind of reputation (table 2). Finally, if no information is available a default value is used, which can be regarded as some Confidence value.

Table 2 shows how electronic market places like eBay can be represented within our general framework. The Trust of a buyer b_1 in the ability of a seller s_1 is built upon the direct experience they had during the transaction. Another buyer b_2 can establish its Witness-Reputation based on the rating b_1 gave to s_1 during their common experience. In eBay's system, this rating can be found in the corresponding line in s_1's transaction history. Finally, the Neighbor-Reputation is made with the aggregation of ratings from various buyers. To use the same example (eBay) the global value, computed for the overall transactions of a seller, can be used.

SOCIAL REGRET does not represent the "unknown" state, when an agent do not know how to judge another one, generally due to a lack of experiences. As it is shown in section 3.2 it may, however, prove really important in some cases (like in the openness problem).

4.2 In Social Sciences

CONTE and PAOLUCCI study reputation in human society. Their model uses three roles: Evaluators, Targets, Beneficiary and the process of Gossip ([3]). The process of Gossip is particularly studied and two specific rules seems to emerge in our society.

It seems obvious that this model can be represented within our framework (see section 2). Indeed, the "Evaluators" role in CONTE and PAOLUCCI's model is simply a merge of the roles labeled "Evaluators", "Observers" and "Gossipers" in our model.

The process of "Gossip" they are attached to describe precisely (since it, in their humble opinion, contribute largely to differentiate their model from Game Theoretical point of view) can be mapped to our different sorts of recommendations processes. However, these rules for gossiping are adapted to our human society and may not apply to the problem of openness in distributed systems, so theses precise rules may not be the most efficient ones is our case.

Conclusion and Future Work

A formal and general model of trust-related topics have been described. Some applications of this model to existing e-commerce and Social Sciences systems have been briefly presented. Meanwhile, as we claim that this model is general and robust, we need to find more and more applications to apply our model to in order to prove it.

Moreover, since the model has been described in terms of agents and roles, it would be really interesting to reformulate it in a mutli-agent organizational model. For example, the MOÏSE+ model ([7]), which assigns a job to each role and some obligations or permissions associated to those jobs, seems to be a really promising tool.

The aim of our work being to compute a trust service within our fully decentralized and open platform, we need to formulate equations from our model to weight the different concepts of trust, reputations and confidence (like it is done in [16]) and to test some recommendation rules (gossip). Indeed, we assume that if there are different rules in our human societies (e.g. the "prudence" one in [3].), and that they are not simultaneously applicable, that is because they apply to different situations. So, we need to determine which rule(s) will apply in our case.

It is also considered to use suspicion to represent the way reputation should increase (respectively decrease). For example, if an agent has a great trust in an other and that this other agent is badly reputed, then the first agent will increase its suspicion. Then, if the second agent cheats, the decrease of the trust value will be proportional to the (new) suspicion value.

Finally, it is considered to use a process based on a dependence theory; in one case to discover relations of agents **X** believes to be cheaters (respectively, to discover relations of the relations of **X**) to be aware of them possibly cheating

Point of View (Beneficiary)	Evaluator	Target	Gossiper	Observer	attribute
b_1	b_1	s_1	Internet Web-site	b_1	$Trust(s_1, \alpha)$
b_2	b_1	s_1	Internet Web-site	b_1 $(b_1 \in \mathcal{O} \Rightarrow b_1 \in \mathcal{W})$	$WR_p(s_1, \alpha)$
b_2	$\mathcal{B}$	s_1	Internet Web-site	$\mathcal{B}$	$NR_p(s_1, \alpha)$

Table 2: eBay-like Systems represented within the general framework. The "inputs" come from past transactions. b_1 bought an article to s_1. α is the ability to buy. $\mathcal{O}$ (resp. $\mathcal{W}$) is the set containing the agents playing the role "Observer" (resp. "Witness"). $\mathcal{B}$ is a subset of the buyers.

on it (respectively, to have an *a priori* idea about those unknown agents). In the other case, the theory may be used during the gossip process, to select agents which opinions **X** will take care of. Indeed, let's suppose there is one agent "pro-agent **Y**" and three agents "con-agent **Y**". If the group of three is in close relation, then taking into account all the ratings, with a weight of a quarter each, will not give a final fair rating of **Y**.

5. REFERENCES

[1] C. Castelfranchi and R. Falcone. Principles of trust in mas: Cognitive anatomy, social importance, and quantification. In *Proceedings of ICMAS'98*, pages 72–79, 1998.

[2] C. Castelfranchi and R. Pedone. A review on trust in information technology. http://alfebiite.ee.ic.ac.uk/docs/papers/D1/ab-d1-cas+ped-trust.pdf.

[3] R. Conte and M. Paolucci. *Reputation in Artificial Societies. Social Beliefs for Social Order*. Kluwer Academic Publishers, 2002.

[4] C. Dellarocas. Analyzing the economic efficiency of eBay-like online reputation reporting mechanisms. In *Proceedings of the 3rd ACM Conference on Electronic Commerce (EC-01)*, pages 171–179, New York, October 14–17 2001. ACM Press.

[5] T. Grandison. Trust specification and analysis for internet applications.

[6] N. Guibert. La confiance en marketing : fondements et applications. In *Recherche et Applications en Marketing*, volume 14, 1999.

[7] M. Hannoun. *MOISE: A Model for Representing Organizations in MAS*. PhD thesis, École des Mines de Saint-Étienne, 2003.

[8] N. Luhmann. *Trust and Power*. John Wiley and sons, 1979.

[9] D.H. McKnight and N.L. Chervany. *Trust in Cyber-societies*, chapter Trust and Distrust Definitions: One Bite at a Time, pages 27–54. Springler-Verlag Berlin Heidelberg, 2001.

[10] L. Mui and M. Mohtashemi. Notions of reputation in multi-agent systems: A review. In *AAMAS'2002 and MIT LCS Memorandum*, 2002.

[11] E. Orstom. Aa behavioral approah to the rational-choice theory of collective action. *American Political Science Review*, 1998.

[12] L. Quéré. La structure cognitive et normative de la confiance, 2003.

[13] J. Rouchier. *La confiance à travers l'échange. Accès aux pturages au Nord-Cameroun et échanges non-marchands : des simulations dans des systèmes multi-agents*. PhD thesis, Université d'Orleans, 2000.

[14] J. Sabater and C. Sierra. Regret: A reputation model for gregarious societies, 2000. http://www.citeseer.nj.nec.com/sabater00regret.html.

[15] J. Sabater and C. Sierra. Reputation and social network analysis in multi-agent systems. In *Proceedings of AAMAS'02*, page 9, 2002.

[16] J. Sabater and C. Sierra. Social regret, a reputation model based on social relations. *SIGecom Exchanges. ACM*, 3.1:44–56, 2002. http://www.acm.org/sigecom/exchanges/volume_3_(02)/3.1-Sabater.pdf.

[17] S. Sen and N. Sajja. Robustness of reputation-based trust: boolean case. In *AAMAS 2002*, pages 288–293, 2002.

[18] C. Tardieu. La confiance envers le site web d'une entreprise. comment inspirer confiance et engager une relation dans le long terme avec les internates ?, 2000. http://perso.wanadoo.fr/cybermarketing/confiance.htm.

[19] L. Vercouter. *Engineering Societies in the Agents' World II*, chapter A distributed approach to design open multi-agent systems, pages 25–38. LNAI 2203. Springer, 2001.

[20] Bin Yu and M.P. Singh. An evidential model of distributed reputation management. In *Proceedings of First International Joint Conference on Autonomous Agents and Multi-Agent Systems*, pages pages 294–301, 2002.

[21] G. Zacharia, A. Moukas, and P. Maes. Collaborative reputation mechanisms in electronic market places. In *Proceedings of the 32nd Hawaii International Conference on System Sciences*, 1999.