2007-9

Temporal Factors to evaluate trustworthiness of virtual identities

Luca Longo
Technological University Dublin, luca.longo@tudublin.ie

Pierpaolo Dondio
Technological University Dublin

Stephen Barrett
Technological University Dublin

Recommended Citation

L. Longo, P. Dondio and S. Barrett, "Temporal factors to evaluate trustworthiness of virtual identities," 2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm 2007, 2007, pp. 11-19, doi: 10.1109/SECCOM.2007.4550300.

Temporal Factors to evaluate trustworthiness of virtual identities

Luca Longo, Pierpaolo Dondio, Stephen Barrett
School of Computer Science and Statistics, Distributed System Group,
Trinity College Dublin, College Green 2, Dublin
longo.luca@gmail.com dondiop@cs.tcd.ie stephen.barrett@cs.tcd.ie

***Abstract*—In this paper we investigate how temporal factors (i.e. factors computed by considering only the time-distribution of interactions) can be used as an evidence of an entity's trustworthiness. While reputation and direct experience are the two most widely used sources of trust in applications, we believe that new sources of evidence and new applications should be investigated [1]. Moreover, while these two classical techniques are based on evaluating the outcomes of interactions (direct or indirect), temporal factors are based on quantitative analysis, representing an alternative way of assessing trust. Our presumption is that, even with this limited information, temporal factors could be a plausible evidence of trust that might be aggregated with more traditional sources. After defining our formal model of four main temporal factors - activity, presence, regularity, frequency, we performed an evaluation over the Wikipedia project, considering more than 12000 users and 94000 articles. Our encouraging results show how, based solely on temporal factors, plausible trust decisions can be achieved.**

I. Introduction

In this paper we investigate how temporal factors (i.e. factors computed considering only the time-distribution of interactions) can be used as an evidence of entity's trustworthiness. We hypothesise that temporal factors like *degree of activity, presence, regularity and frequency of interactions* can be meaningful used in a trust computation. In this paper we believe trust factors could be promising in assessing the trustworthiness of virtual identities interacting in an open environment. Since in these environments it is easy to create, change and delete identities, the fact that a virtual identity shows temporal stability and continuous activity appears an interesting property.From an intuitive point of view, the fact that an entity has been around for a long time, always present, active and interacting with regularity enforces the perception that it may have some attributes like stability, a certain skills, transparency, experience, the ability to fulfil expectations; all characteristics that may be linked to the fuzzy notion of trust. The question discussed in this paper is to investigate this hypothesis and to understand if it can help in making trust-based decision. In order to understand all the motivations behind our work, we briefly introduce some issues related to Computational Trust, where this work should be placed. Computational Trust was introduced more than a decade ago when Stephen Marsh [2] proposed the first computational model of trust in a DAI environment (Distributed Artificial Intelligence). Computational trust seeks to apply the human notion of trust in the digital world. The expected benefits, according to Marsh and al., are a *reduction of complexity* (by considering only trustworthy possibilities), the possibility of exploiting others' ability with delegation, the possibility of having more cooperation in open and unprotected environment. A trust-based decision in a specific domain is a multi-stage process. The first step is the identification and selection of the appropriate input data, the trust evidences. These are in general domain-specific and the result of an analysis conducted over the application involved. Then a trust computation is performed over evidences to produce trust values, the estimation of the trustworthiness of entities in that particular domain. The selection of evidences and the subsequent trust computation are informed by a notion of trust, the trust model. Finally, the actual trust decision is taken considering computed values and exogenous factors, like disposition or risk assessments.

Although research in Computational Trust has been underway more than ten years, many authors, notably [1] still write that "many new evidence should be investigated and new application should be considered". It seems clear that the two main sources of trust, explored in depth so far, are direct experience and recommendations (i.e. indirect experience). These two trust evidences are undoubtedly important and effective as many applications have successfully demonstrated, but not a lot remains beyond these two approaches. In this sense, we are in the line of work of Castelfranchi and Falcone [3], that, in their cognitive model of trust, investigate many other components of trust. We underline that our model is not a cognitive approach, but we share the same aim to investigate a new set of evidence in trust.

The concept of trust described in this paper is one where trust is human related and it has a presumptive nature, that is, it is made of simple presumptions to be tested in the context rather than a complex analytical model [4]. Our contribution is to investigate the application of a new presumption, the temporal factors.We believe that temporal factors could be an evidence to be compared to or aggregated with more traditional approaches like direct and indirect experience, in order to obtain a deeper and more useful trust decision. A useful property of temporal factors is that they are based only on quantitative re-elaboration of data. This makes

them easy to compute with no or limited domain-specific expertise and without requiring any feedback. Direct and indirect experience are, on the contrary, based on evaluating the outcomes of (past) interactions and thus could require a qualitative analysis, domain-specific expertise or users presence in the system.

The main drawback of temporal factor is the amount of information required, that in some environments could be hard to gather. However, many applications and scenarios remain suitable for our analysis. Another drawback is that values computed may not carry any useful information, since it may be the case that in certain domains a qualitative analysis is needed in order to asses trust. Clearly temporal factors are based only on a subset of the information that we should know in order to make a decision. In this paper we limit ourselves to the question of whether with this small subset of information, it is possible to help the decision making process. In this paper we will present an evaluation of our temporal factors over the Wikipedia project. In this scenario, we test if temporal factors could help us to identify reliable and trustworthy virtual authors, on the basis of their editing activity over time. As described above, we will not consider what an author wrote in his contributions to Wikipedia, but only when he did his contributions. The paper is organized as follows: section 2 describes some related works, section 3 shows our model of trust temporal factors called LTTM, including informal and formal definition. Section 4 describes base functions of LTTM and section 5 formalizes trust factors. Section 6 describes trust function and section 7 contains an example of the model application. In the section 8 there is our evaluation while the last section contains our conclusions and future works.

II. Related Works

There are many definitions of the human notion of trust in a wide range of domains from sociology, psychology to political and business science and these definitions may even change when the application domain change. For example, Romano's recent definition tries to encompass the previous work in all these domains: "Trust is a subjective assessment of another's influence in terms of the extent of one's perception about the quality and significance of another's impact over one's outcomes in a given situation, such that one's expectation of, openness to, and inclination toward such influence provide a sense of control over the potential outcomes of the situation". This sections illustrates works relevant to all or some aspects covered in this paper: previous application of Computational Trust in the context of the Wikipedia project; literature supporting the use of time-dependent information for supporting trust; the problem of the reliability of virtual identity and a brief overview of evidence selection in trust. In the context of computational trust the problem of Wikipedia trustworthiness has been already studied by few authors. Dondio et Al. [5] performed a set of experiments by mapping onto a model of Wikipedia expertise derived from studies in *collaborative editing* and *content quality*. They identified a set of trust evidence justified by experts and mapped into elements of Wikipedia. A second set of experiments [4], [6] was performed by applying a set of generic trust schemes onto Wikipedia, described as a set of generic reasons to trust an entity. The results obtained were compared to the expert-based approach. Two of these generic trust schemes, namely *stability* and *persistence*, are clearly linked to temporal factors and are complementary to the ones presented here. Mc Guiness [7] performed a trust computation over Wikipedia by applying a citation-based algorithm, considering the links structure among Wikipedia articles. Finally, Zeng et al. [8] considered the history of revisions of a Wikipedia article as trust evidence and then they computed trust values using a Bayesian trust model.

Literature supporting the role of temporal factors in trust evaluation is broad. Pickett and Sussman [9] studied the causal attribution between stability and trustworthiness in a complex cognitive framework involving the concept of credibility and objectivity as well. Frewer and Miles in [10] showed how presence and constant activity is directly linked to perceived trustworthiness. Different bodies - public and private - were asked to release the same information regarding some food hazards. The sample of people involved in the test tended to consider the information more trustworthy if given by a body with temporal stability. For example, hospitals had a higher consideration than governments, considered a more volatile entities. This proved that humans consider stability and trust correlated. The Standford Persuasive Labs Guidelines [11] attributes to the permanence of the information on the Web over time one of the main five sources of credibility and trust. The problem of trustworthiness of virtual identity is a well investigated problem with a variety of solutions. Some authors, notably Seigneur and Damsgaard [12] noticed how the problem of virtual identity is linked to the problem of privacy. In order to asses trustworthiness, we may need to gather information that may compromise the privacy of the users behind the virtual identity. However, one of the main rationale for using virtual identities and pseudonyms is to keep privacy. Thus, there is a trade-off between privacy and trust and the authors suggests that a solution to this problem should allow the benefit of adjunct trust when entities interact without too much privacy loss. In respect to this, our temporal factors doesn't reveal anything regarding the person beyond a virtual identities but are based exclusively on its activity in the virtual environment. Certanly, the knowledge of interactions time-distribution represents a set of information that may reduce entity's privacy, but we consider this relatively minimal.

Friedman and Resnick [13] pointed out that, even in the physical world, name changes have always been possible as a way to erase one reputation. The Internet highlights the issue, by making name changes almost cost-free. The authors said that this creates a situation where positive

reputations are valuable, but negative reputations do not stick (are easy to delete) that supports the hypothesis that presence and persistence over time enforces trust. The authors propose a different solution to this problem: the use of entry fees (associated with each personal identifier), a time consuming registration process, or to give people the option of committing not to change identifiers, that means each person is given a single identifier that is unrelated to the person's true identity that could not be changed and called once-in-a-liftetime identifiers.

The EU project SECURE [14] represents an example of an evidence-based trust engine, that defines trust in terms of past evidence, but also uses a recommendation system, a policy language and a risk management module. Recommendations systems [15] typically advise people of products they might appreciate, taking into account their past ratings' profile and history of purchase or interest. Examples of these include ebay.com, amazon.com and epinions.com. In these systems trust is calculated by each user according to their personal judgments: we exploit and propagate trust calculations made in users' mind. Golbeck [16] studied the problem of propagating trust value in social network, by proposing an extension of the FOAF vocabulary and algorithms to propagate trust values. The community of users is a graph where nodes (users) are connected with oriented links that have a trust value as their weighs. Again, the focus of the research is not about how to calculate trust value (the user inserts this) but its distribution and propagation. Ziegler [17] studied interesting correlation between similarity and trust among social network users. It is relevant as an example of similarity as an evidence of trust. In both social networks and recommendation systems, trust is seen as a value (fuzzy or crisp) that is subjective and can be composed transitively.

Trust is human-based: the key hypothesis is that the domain should allow communication and retrieval of recommendations and recommenders. Some mathematical and probabilistic approaches have been explored also. Wang [18] applies Bayesian Network theory to study the trustworthiness of a P2P file sharing application. Trust is calculated over behaviours, modelled as probability distributions, giving trust calculations an immediate and precise meaning.

III. Definition of L.T.T.M.

A. Informal definition

LTTM (*Longo's Temporal Trust Model*) is a model of trust applicable to a multiagent environment and not to a single agent one since there are many autonomous entities. LTTM field is *completely observable* because each agent has access to the complete state of the system in every moment and as a consequence it can take into account all the most important aspects in order to do a specific action. For example it is possible that an agent α wants to know the level of trust/reputation of an agent β involved in this system before doing a specific action. LTTM provides some factors properly combined by a *trust function* which compute trust/reputation value for a specific agent. These environments prove to be convenient because agents don't have to save an internal state of the system. Thanks to this feature LTTM is a model that can be easily applicable to virtual environments such as internet virtual communities.

LTTM works in a *stochastic* rather than a deterministic environment since the following state of the system is neither entirely based on the current state nor determined by an action done by an agent: as a consequence it is not possible to guarantee the predictability of the state. LTTM foresees that the state of the system, in a certain instant of time, is formed by the set of agents and by the interactions occurred between them. LTTM models a *episodic operating* environment and the agent experience is divided into atomic events. Each event consists in the perception by the agent which is followed by the execution of a single action. The crucial aspect is that the choice of action depends only on the current event and not a prior history of events. LTTM works in a *dynamic* environment and not in a static context because the system state can change while an agent is thinking. The cardinality of the agents involved in the system can vary with time after their association or dissociation with the system.

So LTTM Model works in a multiagent and entirely observable, stochastic, episodic, dynamic environment. The model can be seen as a graph that evolves in time with dynamism and whose vertex represent the agents involved in the system and its arcs model the interactions that happen. Moreover the interactions are labelled with the temporal value in which the interaction between two agents occurred since the time factor is crucial in this model.

B. Formal Definition

A LTTM *L* is a 7-tuple whose components have the following meanings:

$$L =< A,\ T,\ \Phi,\ \Delta,\ \pi, AG_{sys},\ \tau_0 >$$

- $A \subseteq \aleph$: agents set;
- $T \subseteq \aleph$: time domain;
- $\Phi \subseteq A \times T \times A$: interactions table;
- $\Delta : A \rightarrow \Re$: trust function;
- $\pi \in T$: awaited frequency constant;
- $AG_{sys} \in A$: system agent;
- $\tau_0 \in T$: system validity beginning.

C. Model Working

LTTM works in a dynamic environment because as a new agent associates with the system, the cardinality of the set A increases. T set represents the *time domain* in which there are infinite temporal values, usually modelled with timestamps. The *awaited frequency constant* π is a temporal value belonging to T set that indicates an interval within which at least an interaction by every agents towards other agents is waited. A

tuple such as (α, τ, β) models an interaction occurred between agent α and agent β at τ instant. More precisely α marks the source agent, that is, the agent that has started the interaction towards the target agent β. AG_{sys} is a special agent belonging to the A set that is responsible for the starting of the system at τ_0 time that belongs to *time domain* T. It is also a target agent of a special interaction called *initialization interaction* which allows new agents to associate to the system in an instant of time that is larger than τ_0. Φ models the collection of interactions occurred in the system beginning from τ_0 instant that means the set of tuples such as (α, τ, β). Finally Δ represents the *trust function* that gives trust/reputation value of a specific agent back.

IV. Base Functions

Before defining trust-factors to compute trust value of an agent, it needs to formally define some *base-functions*.

A. Cardinality Function

$$\begin{gathered} C_{ard} : \Phi \to \aleph \\ C_{ard}(\varphi) = \mid \varphi \mid \end{gathered} \tag{1}$$

It returns the cardinality of the input set, that is, the number of the (α, τ, β) tuples hold by it.

B. Time Function

$$\begin{gathered} T_{ime} : \Phi \to T \\ T_{ime}((\alpha, \tau, \beta)) = \tau \end{gathered} \tag{2}$$

It returns the τ value of the (α, τ, β) tuple in input that means the time in which is happened the interaction between the α agent and the β agent.

C. Source Function

$$\begin{gathered} S_{ource} : \Phi \to A \\ S_{ource}((\alpha, \tau, \beta)) = \alpha \end{gathered} \tag{3}$$

It returns the α value of the (α, τ, β) tuple in input, that is, the source agent of the interaction between the α agent and the β agent at time τ.

D. Target Function

$$\begin{gathered} T_{arget} : \Phi \to A \\ T_{arget}((\alpha, \tau, \beta)) = \beta \end{gathered} \tag{4}$$

It returns the β value of the (α, τ, β) tuple in input that means the target agent of the interaction between the α agent and the β agent at time τ.

E. System Life Cycle Function

$$\begin{gathered} LC_{sys} : T \to T \\ LC_{sys}(\upsilon) = \begin{cases} \upsilon - \tau_0 & \text{if } \upsilon \geq \tau_0 \\ 0 & \text{otherwise} \end{cases} \end{gathered} \tag{5}$$

It returns the system life cycle value, that is, the difference between the υ input value and the τ_0 value if the τ time is greater or equal than the input time, otherwise it returns 0.

F. Agent Born Function

$$\begin{gathered} BD_{ag} : A \to T \\ BD_{ag}(\gamma) = T_{ime}(\{(\alpha, \tau, \beta) \mid \\ (\alpha, \tau, \beta) \in \Phi,\ \alpha = \gamma,\ \beta = AG_{sys}\}) \end{gathered} \tag{6}$$

It returns the time in which the γ agent has joined the system that means his born date. The function gets the time of the *initialization interaction* between the γ agent and the *system agent*.

G. Agent Life Cycle Function

$$\begin{gathered} LC_{ag} : A \times T \to T \\ LC_{ag}(\gamma, \upsilon) = \\ \begin{cases} \upsilon - BD_{ag}(\gamma) & \text{if } \upsilon \geq BD_{ag}(\gamma) \\ 0 & \text{otherwise} \end{cases} \end{gathered} \tag{7}$$

It returns the life cycle of the γ agent, that is, the time interval between his born date and υ time value. This function compute the difference between the input υ time value and the *initialization interaction* time value of the γ agent.

H. System Interactions Function

$$\begin{gathered} I_{sys} : T \to \Phi \\ I_{sys}(\upsilon) = \{(\alpha, \tau, \beta) \mid \forall (\alpha, \tau, \beta) \in \Phi, \\ \tau_0 < \tau \leq \upsilon,\ \beta \neq AG_{sys},\ \alpha \neq AG_{sys}\} \end{gathered} \tag{8}$$

It returns the $(\alpha, \upsilon, \beta)$ tuples set of the system happened in the interval $[\tau_0, \upsilon]$. This set doesn't hold the *initialization interactions* of agents.

I. Interval Agent Input Interactions Function

$$\begin{gathered} I_{ag}^{IN_a^b} : A \times T \times T \to \Phi \\ I_{ag}^{IN_a^b}(\gamma, \tau_{lower}, \tau_{upper}) = \\ = \{(\alpha, \tau, \beta) \mid \forall (\alpha, \tau, \beta) \in \Phi, \\ \tau_{lower} \leq \tau \leq \tau_{upper},\ \alpha \neq AG_{sys},\ \beta = \gamma\} \end{gathered} \tag{9}$$

It returns the $(\alpha, \upsilon, \beta)$ tuples set of the system happened in the interval $[\tau_{lower}, \tau_{upper}]$ in which α is not the *system agent* and β is the input γ agent. The function returns the input interactions set of the γ agent in a specific interval.

J. Interval Agent Output Interactions Function

$$
\begin{aligned}
&I_{ag}^{OUT_a^b} : A \times T \times T \to \Phi \\
&I_{ag}^{OUT_a^b}(\gamma, \tau_{lower}, \tau_{upper}) = \\
&= \{(\alpha, \tau, \beta) \mid \forall (\alpha, \tau, \beta) \in \Phi, \\
&\tau_{lower} \leq \tau \leq \tau_{upper},\ \alpha = \gamma,\ \beta \neq AG_{sys}\}
\end{aligned} \tag{10}
$$

It returns the $(\alpha, \upsilon, \beta)$ tuples set of the system happened in the interval $[\tau_{lower}, \tau_{upper}]$ in which α is the input γ agent and β is not the *system agent*. The function returns the output interactions set of the γ agent in a specific interval.

K. Presence Function

$$
\begin{aligned}
&P_{res} : A \times T \times T \to [0,1] \subseteq \aleph \\
&P_{res}(\gamma, \tau_{lower}, \tau_{upper}) = \begin{cases} 0 & \text{if } \mu = 0 \\ 1 & \text{if } \mu \geq 0 \end{cases} \\
&\mu = (\ C_{ard}(I_{ag}^{IN_a^b}(\gamma, \tau_{lower}, \tau_{upper})) + \\
&C_{ard}(I_{ag}^{OUT_a^b}(\gamma, \tau_{lower}, \tau_{upper}))\ )
\end{aligned} \tag{11}
$$

It returns 0 if there is no interactions in the interval $[\tau_{lower}, \tau_{upper}]$ otherwise it returns 1, that means there is at least one interaction done in the interval $[\tau_{lower}, \tau_{upper}]$ by agent γ.

V. Trust Factors Definition

In order to define trust factors we need base-functions.

A. Activity Factor

The activity factor computes the activity percentage of the input agent to total system activity at τ time.

$$
\begin{aligned}
&F_{act} : A \times T \to [0,1] \subseteq \Re \\
&F_{act}(\gamma, \upsilon) = \\
&= \begin{cases} \frac{Card(I_{ag}^{IN}(\gamma, \tau_0, \upsilon) + I_{ag}^{OUT}(\gamma, \tau_0, \upsilon))}{Card(I_{sys}(\upsilon))} & \text{if } \upsilon \geq \tau_0 \\ 0 & \text{otherwise} \end{cases}
\end{aligned} \tag{12}
$$

B. Presence Factor

The presence factors returns the presence percentage of the input agent at τ time.

$$
\begin{aligned}
&F_{pres} : A \times T \to [0,1] \subseteq \Re \\
&F_{pres}(\gamma, \upsilon) = \begin{cases} \frac{LC_{ag}(\gamma, \upsilon)}{LC_{sys}(\upsilon)} & \text{if } \upsilon \geq \tau_0 \\ 0 & \text{otherwise} \end{cases}
\end{aligned} \tag{13}
$$

C. π Frequency Factor

The frequency factor computes the frequency percentage of the input agent at τ timeusing π constant. The frequency is the number of input/output interactions of a specific agent to his life cycle. If the frequency with which the input agent interact with other ones is greater or equal than the *awaited frequency constant* π, it means that the agent reflect 100% the *awaited frequency*, otherwise the agent doesn't respect the *awaited frequency constant* π.

$$
\begin{aligned}
&F_{freq}(\gamma, \upsilon) = \begin{cases} 1 & \text{if } \mu \cdot \pi \geq 1 \\ \mu \cdot \pi & \text{otherwise} \end{cases} \\
&F_{freq} : A \times T \to [0,1] \subseteq \Re \\
&\mu = \begin{cases} \frac{Card(I_{ag}^{IN}(\gamma, \tau_0, \upsilon) + I_{ag}^{OUT}(\gamma, \tau_0, \upsilon))}{LC_{ag}(\gamma, \upsilon))} & \text{if } \upsilon \geq \tau_0 \\ 0 & \text{otherwise} \end{cases}
\end{aligned} \tag{14}
$$

D. π Regularity Factor

The regularity factor returns the regularity percentage of the input agent at τ time using π constant. An agent is 100% regular if in each sub-interval, with width π, of the interval $[BD_{ag}, \upsilon]$, there exists at least one interaction with another agent, otherwise it says the agent is irregular. In other words, the system expects that each agent in the Φ set interacts at least once with other agent every π time.

$$
\begin{aligned}
&F_{reg} : A \times T \to [0,1] \subseteq \Re \\
&\lambda = BD_{ag}(\gamma) \\
&\mu = \sum_{\tau=0}^{\lfloor \frac{LC_{ag}(\gamma, \upsilon)}{\pi} \rfloor} \frac{P_{res}(\gamma,\ \lambda + \tau \cdot \pi,\ \lambda + \tau \cdot \pi + \pi)}{\lfloor \frac{LC_{ag}(\gamma, \upsilon)}{\pi} \rfloor} \\
&F_{reg}(\gamma, \upsilon) = \begin{cases} \mu & \text{if } \upsilon \geq \tau_0 \\ 0 & \text{otherwise} \end{cases}
\end{aligned} \tag{15}
$$

VI. Trust Function Δ

The *trust function* Δ is defined using a *priority hierarchy* which associates a specified weight to each trust factors. Each weight is a specific percentage and their sum must be 100%. This feature has been introduced to emphasize some factors rather other ones and it could change in the context modeled.

An example of *priority hierarchy* could be:

- Presence factor: $\frac{1}{3}$;
- Regularity factor: $\frac{1}{4}$;
- Activity factor: $\frac{1}{4}$;
- Frequency factor: $\frac{1}{6}$.

The *trust Function* Δ can be formally defined as:

$$
\begin{aligned}
&\Delta : A \times T \to [0,1] \subseteq \Re \\
&\Delta(\gamma, \upsilon) = \frac{1}{3} \cdot F_{reg}(\gamma, \upsilon)\ +\ \frac{1}{4} \cdot F_{freq}(\gamma, \upsilon)\ + \\
&+\ \frac{1}{4} \cdot F_{act}(\gamma, \upsilon)\ +\ \frac{1}{6} \cdot F_{pres}(\gamma, \upsilon)
\end{aligned} \tag{16}
$$

VII. LTTM Example

Let LTTM $L =< A,\ T,\ \Phi,\ \Delta,\ \pi, AG_{sys},\ \tau_0 >$ with:

- $A = \{0, 1, 2, 3, 4, 5\}$;
- $T = \{1, 2, ..., n\}$;

- $\Phi = \begin{cases} (1,\ 1181316000,\ AG_{sys}) \\ (2,\ 1181505025,\ AG_{sys}) \\ (3,\ 1181534437,\ AG_{sys}) \\ (4,\ 1181598615,\ AG_{sys}) \\ (1,\ 1181898450,\ 4) \\ (5,\ 1181827200,\ AG_{sys}) \\ (3,\ 1182165083,\ 5) \\ (2,\ 1182361508,\ 4) \\ (4,\ 1182367898,\ 2) \\ (2,\ 1182647715,\ 5) \\ (5,\ 1182882312,\ 3) \\ (4,\ 1182882312,\ 5) \end{cases}$;
- $\Delta(\gamma, \upsilon) = \frac{1}{3} \cdot F_{reg}(\gamma, \upsilon) + \frac{1}{4} \cdot F_{freq}(\gamma, \upsilon) + + \frac{1}{4} \cdot F_{act}(\gamma, \upsilon) + \frac{1}{6} \cdot F_{pres}(\gamma, \upsilon)$;
- $\pi = 86400$;
- $AG_{sys} = 0$;
- $\tau_0 = 1181131800$.

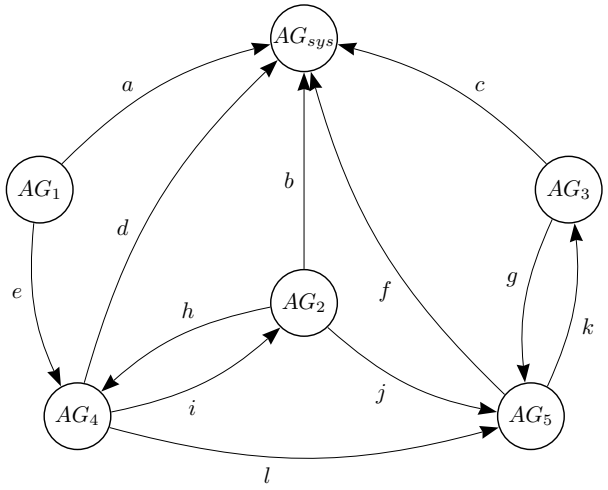

Fig. 1. Graph associated to LTTM L

In this example LTTM models a context with 5 agents plus the *system agent* 0, 12 interactions where 5 are *initialization interactions*. The *awaited frequency constant* π is 86400 seconds that means 1 day and τ_0 is 1181131800 that, in natural language, means $6th\ June$ 2007, 12:10:00 GMT. The graph associated to L is shown in figure 1. Supposing to call the *trust function* for each agent at time $\tau = 1182974400$, that is, $27th\ June$ 2007, 20:00:00 GMT, the results of trust factors and the finals trust values are shown in tables II and III.

VIII. Evaluation

We now report on our experiment over the Wikipedia project. By using our temporal factors, we hope to predict the trustworthiness of Wikipedia authors based on the time-distribution of their contributions. Wikipedia is an online collaborative encyclopaedia written by an open community of users and the problem of its articles trustworthiness has been strongly discussed [19]. Wikipedia makes its data available

Label	Timestamp	Natural Language
a	1181316000	June 8, 2007 15:20:00
b	1181505025	June 10, 2007 19:50:25
c	1181534437	June 11, 2007 04:00:37
d	1181598615	June 11, 2007 21:50:15
e	1181898450	June 14, 2007 13:20:00
f	1181827200	June 15, 2007 09:07:30
g	1182165083	June 18, 2007 11:11:23
h	1182361508	June 20, 2007 17:45:08
i	1182367898	June 20, 2007 19:31:38
j	1182647715	June 24, 2007 01:15:15
k	1182882312	June 26, 2007 18:25:12
l	1182882312	June 27, 2007 10:10:00

TABLE I
TIMESTAMPS IN NATURAL LANGUAGE

γ	$\frac{F_{pres}(\gamma,\tau)}{3}$	$\frac{F_{reg}(\gamma,\tau)}{4}$	$\frac{F_{act}(\gamma,\tau)}{4}$	$\frac{F_{freq}(\gamma,\tau)}{6}$
1	0.3000	0.0131	0.0357	0.0086
2	0.2658	0.0294	0.1071	0.0294
3	0.2604	0.0312	0.0714	0.0201
4	0.2488	0.0333	0.1428	0.0418
5	0.1946	0.0625	0.1428	0.0535

TABLE II
TRUST FACTORS RESULTS

for downloading and this support statistical computations. It provides html or xml dumps for all of its sections: current articles, current pages, articles' history, pages' history and the complete text data as well. We chose the xml dump because it is well structured and, for computational reason, we focused our attention on the English *wikisource* section [20] containing novels, non-fiction works, letters, speeches, constitutional and historical documents, laws and a range of other documents. We downloaded the *enwikisource-20070510-stub-meta-history.xml* that stores the complete history of this section, that is, the entire set of revisions done on the *wikisource*'s pages including theirs contributors from 15Th january 2001, the launched date of the Wikipedia's English edition [21], to 10Th May 2007.

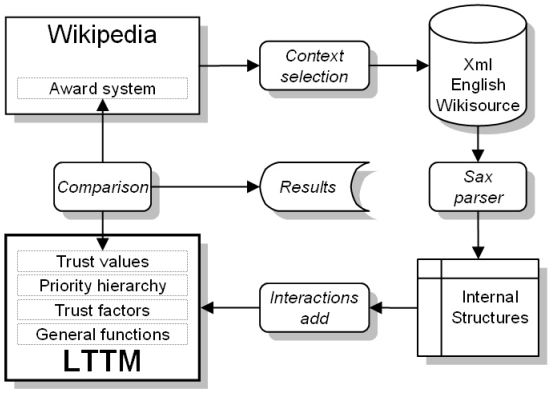

Fig. 2. Prototype's logical view

γ	$\Delta(\gamma,\tau)$	%
1	0.35756612	$35,75\%$
2	0.4317704	$43,17\&$
3	0.38317385	$38,31\%$
4	0.46694222	$46,69\%$
5	0.45353466	$45,35\%$

TABLE III
TRUST RESULTS

#	π	$Trust\ average\ (\psi)$	$Standard\ deviation\ (\omega)$	(ω/ψ)
1	1	$5,74\%$	4.6%	80.3%
2	3	$7,29\%$	6.3%	86.4%
3	7	$9,43\%$	7.8%	83.2%
4	31	$16,97\%$	10.8%	64.1%

TABLE IV
TRUST AVERAGES AND STANDARD DEVIATIONS

We wrote a prototype of LTTM formal model using Java [22]. We have built a specific package whose logical view is shown in figure 2. The prototype analyses the xml file, downloaded from Wikipedia's server, using Sax technology. Sax is an event driven parser that registers one listener and parsers Xml file notifying Xml found elements. During this step the prototype creates its own data structures in order to save information about Wikipedia's pages, revisions and their contributors: a typical Xml Wikipedia's file is shown in figure 3.

```
...
<page>
 <title>Main Page</title>
 <id> 2 </id>
 <revision>
  <id> 23 </id>
  <restrictions>move=sysop:edit=sysop</restrictions>
  <timestamp> 2003-11-23T23:51:22Z </timestamp>
  <contributor>
   <ip> 201.123.456.88 </ip>
  </contributor>
  <text xml:space="preserve"> text </text>
 </revision>
 <revision>
  <id> 67 </id>
  <timestamp> 2006-10-29T}01:23:51Z </timestamp>
  <contributor>
   <username> Luca </username>
   <id> 6079 </id>
  </contributor>
  <minor />
  <comment> text </comment>
  <text xml:space="preserve"> text </text>
 </revision>
 ...
</page>
...
```

Fig. 3. Wikipedia's Xml file structure

In the next step an istance of LTTM model is populated by inserting agents and interactions. In the Wikipedia context we consider agents both the pages (passive agents) and the contributors (active agents) while interactions are the Wikipedia's revisions done by contributors over pages. A typical interaction tuple is <Contributor, Revision's date, Page> that indicates the interaction between a specific "Contributor" and "Page" at the "Revision's date". The *enwikisource-20070510-stub-metahistory.xml* file contains 94251 pages and 329639 revisions thus it can be a meaningful data set. At the end of the parsering step we identified 12354 users with at least one revision done. Considering these data, LTTM model will contain $94251 + 12354 = 106605$ *agents* so 106605 *initialization interactions* and 329639 *interactions*.

In Wikipedia's context we presume that our *presence factor* is an indicator of user experience, our *activity*, *frequency* and *regularity* factors emphasizes agents having more regular interactions, that could be regarded as an agent's care of Wikipedia (there are actually many extreme Wikipedians that really cares the encyclopedia). In our experiment we set the priority hierarchy with equals factors's weights ($\frac{1}{4}$ each): the study of an optimal hierarchy priority is not a goal of this experiment.

The first step of our experimentation is to understand the importance of the π constant (awaited frequency constant) essential for computing all the temporal factors. We performed a set of computations changing the π constant (in days, i.e., $86400\times$ value) obtaining trust averages and standard deviation values shown in table IV and in figure 4.The higher the π value, the more the average percentage of the 12354 users increases. This is not enough to understand the effect of changing π, since if the trust values increase for all the users in the same manner the results are exactly the same. If we take in consideration the ratio average/standard deviation we clearly notice that the value is almost stable for the first three cases and it strongly decreases for the last case. This means that when π has high values (like 31 days) the results have less variance and thus they tend to be more similar and less selective. The interpretation is that the value of π is so high that much more users can be considered present and regular. This means that many users show high trust value, making this value less effective for dividing bad and good cases.

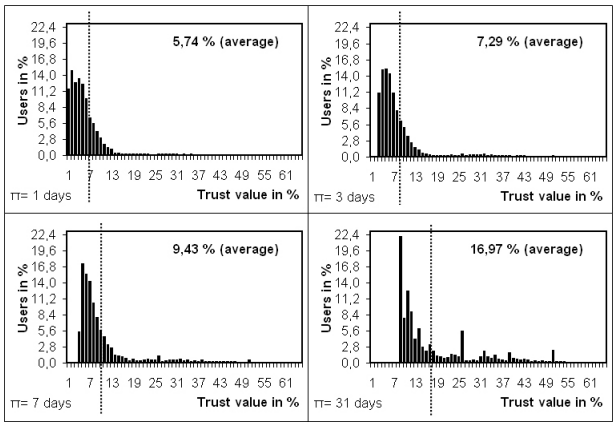

Fig. 4. 12354 "Enwikisource"'s users with LTTM trust value

Wikipedia uses awards in a non-automatic way to recognise particularly valuable contributors to the encylopaedia. One of this is the "Original Barnstar Award" given to let people know that their hard work is seen and appreciated. This award is given at users discrection to another user simply adding on his page the web-link of the "Original Barnstar Award". The Wikipedia's English edition has a list of people that have been awarded a "barnstar". Since we are considering only the "wikisource" section, some of the users in the list couldn't have taken part in any revision. In fact we have identified just 70 users on 500 of the list that have contributed at least to one article in the subset of interest.

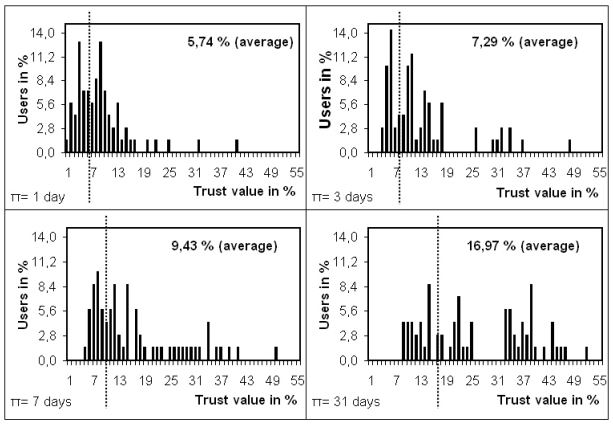

Fig. 5. 70 "Enwikisource"'s awarded users with LTTM trust value

In this work, our hypothesis is that time-dependant factors can be consider as trust evidence. In order to test this in the Wikipedia context, we analyse if users awarded by Wikipedia show higher trust values than the standard users ones. We have to recall that our model is formal and automatic whereas in Wikipedia, the assignement of trust values rests entirely on the discretion of the users community. Given that, it might be the case that some authors with a very high LTTM value don't may not have an award. The user must receive the award nevertheless if our method has merit.

The results are presented in figure 4 and 5. The figure 5 shows the distribution of the % of the Wikipedia's awarded users by their trust value computed by LTTM for 4 different values of π constant. Results obtained by our model are encouraging and positive. We can see that the majority of the users are on the right side of the average (dashed line). This means that the majority of the users indicated by Wikipedia as good users by "Original barnstar award" have been actually recognised by LTTM model as good users as well (an average rate of good prediction around 70%).

We notice that a very few awarded users (around 10%) has a very low LTTM trust value. Anyway, our model doesn't succeed for this portion of users so, in this case, others trust evidences should be considered before taking decisions. Our results are not yet validated. Only by comparing the distribution of awarded authors and the distribution of normal authors it is possible to validate our conclusions: if distributions show significant differences this means that LTTM was effective in identifying good authors. Figure 4 shows the distributions of all the 12354 users. It is clear how the distribution of normal users shows difference with the one presented in figure 5 and it enforces our results. The majority of authors is concentrated around the average, showing a more compact (and thus less effective) distribution than the awarded users one.

Distinctive sign	Users	%
Very active user who show his contributions in his own home page	8	26,6%
EnWikiSource administrator	7	23,5%
Particolars user as professor, sectorial expert or Barnstars awarded	4	13,3%
Ip address shared by multiple users of an educational institution	3	10,0%
User who built a specific tool or started a new project	3	10,0%
Bot	2	6,6%
Not found	2	6,6%
User identified as vandal	1	3,4%

TABLE V
LTTM'S TOP 30 USERS MANUALLY CHECKED

Distinctive sign	Users	%
Anonymous user identified by an ip address	24	80,0%
Inactive user	3	10,0%
User identified as vandal because of his distruptive edits	3	10,0%

TABLE VI
LTTM'S WORST 30 USERS MANUALLY CHECKED

Finally, we manually examined who actually are the top 30 users computed by LTTM on the Wikipedia's web site. We have chose the case #1 and we discovered interesting results shown in table V. As we can see, the majority of the users are administrators, very active users or experts of specific field. We also did the opposite check and we manually analysed the 30 worst users computed by LTTM on the Wikipedia's web site. We expected to find users with a low interest in Wikipedia's life and quality. Actually, the majority of those are anonymous users, or user identified by the community as vandals: the detailed results shown in table VI sustain our thesis and confirm that LTTM model has a promising general validity.

IX. Conclusions and Future Works

In this paper we investigated the usage of temporal factors as an evidence of virtual identities trustworthiness. We began by defining a formal model of four temporal factors: activity, regularity, presence and presence, all defined using only the time-distribution of interactions. Our evaluation was conducted in the context of the Wikipedia project, covering more than 12 000 users and 94 000 articles. We tested our factors against Wikipedia awards system, that assigns a special recognition to reliable and trustworthy authors. The results obtained are encouraging, with a good predictions rate of more than 60% and a bad prediction rate of less than 20%. This shows how temporal factors, even if they are based on a limited set of information, could be effective in supporting a trust decision. We believe that these factors could be a new trust evidence to be aggregated with more traditional ones like past direct experience and recommendation, based on outcomes of interactions analysis.In our future works we will address the crucial problem of understanding the generic conditions that an environment (domain, application) should satisfy in order to assure that temporal factors are in that context a strong and plausible evidence for trust.

References

[1] Seigneur J.M., Ambitrust? *Immutable and Context Aware Trust Fusion.* Technical Report, Univ. of Geneva, 2006

[2] Marsh, S. 1994. *Formalizing Trust as a Computational Concept.* PhD thesis, University of Stirling, Department of Computer Science and Mathematics

[3] Castelfranchi, C., Falcone, R.. *Trust is much more than subjective probability: Mental components and sources of trust*. 32nd Hawaii International Conference on System Sciences, 2000.

[4] Dondio P., Barrett S., *Presumptive Selection of Trust Evidence*. AAMAS 2007, 6th international conference on Autonomous and Multi-Agent Systems, Honolulu, Hawaii, May 2007.

[5] Dondio P., Barrett S., Weber S., Seigneur J.M., *Extracting trust from domain analysis: a study on Wikipedia*, IEEE ATC, Wuhan, China, 2006

[6] Dondio P., Barrett S., *Presumptive Selection of Trust Evidences: a non Invasive, Application-Contained Solution*. IEEE Ubisafe 2007, Niagara Falls, Canada, May 2007

[7] McGuiness, D. et al. *Investigations into Trust for Collaborative Information Repositories: A Wikipedia Case Study*. MTW 06, Edinburgh, Scotland, 2006

[8] H. Zeng et al. *Computing Trust from Revision History*, PST 2006, international conference on Privacy, Security and Trust, Canada, 2006

[9] T. Pickett, L. Sussman. *Causal Attributions and Perceived Source Credibility: Theory, Data, and Implications*, ERCIM Database, Code ED131509, 1976

[10] L. J. Frewer , S. Miles. *Temporal stability of the psychological determinants of trust: Implications for communication about food risks Health*, Taylor and Francis Group, Risk and Society, vol 5 n. 3, 2003

[11] Standford Web Credibility Guidelines. http://credibility.stanford.edu/guidelines

[12] Seigneur, J.M. & Jensen, C.D. (2004). *Trading Privacy for Trust*. Trust Management, Second International Conference iTrust 2004, Oxford, UK, March 29 - April 1, 2004, Proceedings. Lecture Notes in Computer Science 2995, Springer.

[13] Friedman, E.J. & Resnick, P. (1999). *The Social Cost of Cheap Pseudonyms*. Journal of Economics and Management Strategy 10(2): 173-199.

[14] Cahill, V. et al., 2003. *Using Trust for Secure Collaboration in Uncertain Environments*. IEEE Pervasive Computing Magazine, July-September 2003

[15] Resnick P., Varian H., 1997. *Recommender systems*. Communications of the ACM, 40(3):56?58, 1997. ISSN 0001-0782-

[16] Golbeck, J. et al., 2002. *Trust Networks on the Semantic Web*, University of Maryland, College Park.

[17] Ziegler, C., Golbeck, J., 2005. *Investigating Correlations of Trust and Interest Similarity - Do Birds of a Feather Really Flock Together?* To appear in Decision Support Systems, 2005.

[18] Wang, Y., Vassileva, J., 2003. *Bayesian Network-Based Trust Model*, Proc. of IEEE International Conference on Web Intelligence (WI 2003), October 13-17, 2003, Halifax, Canada

[19] Trustcomp Group, http://www.trustcomp.org

[20] English Wikisource, http://en.wikisource.org

[21] English Wikipedia Edition, http://en.wikipeedia.org/wiki/Wikipedia

[22] Java http://java.sun.com

[23] Sax, Simple API for Xml http://java.sun.com/webservices/jaxp/