Trust Evaluation of a System for an Activity

Nagham Alhadad, Patricia Serrano-Alvarado, Yann Busnel, Philippe Lamarre

Trust Evaluation of a System for an Activity

Nagham Alhadad[1], Patricia Serrano-Alvarado[1], Yann Busnel[1], Philippe Lamarre[2]

[1] LINA/Université de Nantes – France
[2] LIRIS/INSA Lyon – France

Abstract. When users need to perform a digital activity, they evaluate available systems according to their functionality, ease of use, QoS, and/or economical aspects. Recently, trust has become another key factor for such evaluation. Two main issues arise in the trust management research community. First, how to define the trust in an entity, knowing that this can be a person, a digital or a physical resource. Second, how to evaluate such value of trust in a system as a whole for a particular activity. Defining and evaluating trust in systems is an open problem because there is no consensus on the used approach. In this work we propose an approach applicable to any kind of system. The distinctive feature of our proposal is that, besides taking into account the trust in the different entities the user depends on to perform an activity, it takes into consideration the architecture of the system to determine its trust level. Our goal is to enable users to have a personal comparison between different systems for the same application needs and to choose the one satisfying their expectations. This paper introduces our approach, which is based on probability theory, and presents ongoing results.

1 Introduction

Everyday digital activities like chatting, mailing, blogging, buying online, and sharing data are achieved through systems composed of physical and digital resources (*e.g.,* servers, software components, networks, data, and personal computers). These resources are provided and controlled by persons (individual or legal entities) on whom we depend to execute these activities. The set of entities and the different relations between them form a complex system for a specific activity.

When users need to choose a system to perform an activity, they evaluate it considering many criteria: functionality, ease of use, QoS, economical aspects, *etc*. Trust is also a key factor of choice. However, evaluating this trustworthiness is a problematic issue due to the system complexity.

Trust has been widely studied in several aspects of daily life. In the trust management community [1,2,3,4,5,6], two main issues arise: *(i) How to define the trust in an entity, knowing that entities can be persons, digital and physical resources?* Defining the trust in each type of entity naturally is different but mainly depends on *subjective* and *objective* properties [6]. *(ii) How to evaluate such value of trust in a system under a particular context?* This point embodies the main focus of our study. We argue that studying trust in the separate entities that compose a system does not give a picture of how trustworthy a system is as a whole. Indeed, the trust in a system depends on its architecture. Several types of trust have been proposed with different meanings, which are strongly context-dependent. Defining and evaluating trust is still an open problem;

there is no consensus on the approach applicable to systems in general. The aim of our work is to propose an approach applicable to any kind of system.

Inspired by probability theory, the goal of this paper is to evaluate the trust value in a system for an activity that a person wants to perform. The system definition is based on SOCIOPATH [7] which allows to model the architecture of a system by taking into account entities of the social and the digital world involved in an activity. To focus on the trust in the system, the SOCIOPATH model is abstracted in a graph-based view. Levels of trust are then defined for each node in the graph. By combining trust values, we are able to estimate two different granularities of trust, namely, *trust in a path* and *trust in a system*, both for an activity to be performed by a person. Our contribution is named SOCIOTRUST, to evaluate it, we conducted several experiments to analyze the impact of different characteristics of a system on the behavior of the obtained trust values. Experiments realized on both synthetic traces and real data sets allow us to validate the accuracy of our approach.

This paper is organized as follows. Section 2 gives a quick overview of SOCIOPATH. In Section 3, we propose SOCIOTRUST to compute the trust value in a system for an activity. Section 4 presents the experiments that validate the proposed approach. Section 5 presents some related works. Finally, we conclude in Section 6.

2 Overview of SOCIOPATH

The SOCIOPATH meta-model [7] describes a system in terms of the entities that exist in *(i)* the *social world* [1], where *persons* own *physical resources* and *data*, and in *(ii)* the *digital world*, where *instances of data* (including application programs) are stored and *artifacts* (software) are running. SOCIOPATH also describes the relations between the different entities of the two worlds. Enriched with deduction rules, the SOCIOPATH meta-model allows to underline and discover chains of *access* relations between *artifacts*, and *control* relations between *persons* and *digital resources* in a system. The main concepts defined in SOCIOPATH are:

- *minimal path* ($\widehat{\sigma}$); a list that begins with an *actor*, ends with a *data instance* and contains *artifacts* in between. Between each two consecutive elements in this list, there is a relation *access*. A *minimal path* describes a straight way an *actor* achieves an *activity* without passing through cycles.
- *activity* (ω); a task like editing a document, where some restrictions are considered to impose the presence of particular elements in the path. For instance, if a user wants to read a `.doc` document, she must use an *artifact* that can *understand* this type of document (*e.g.,* Microsoft Word or LibreOffice Writer).

Each *artifact* in the path is controlled by at least one *person* and supported by at least one *physical resource*. In SOCIOPATH, the persons who *control* an *artifact* are the persons who *own* a *physical resource* that *supports* the *artifact* or who own some *data* represented by a *data instance* that *supports* the *artifact* (the *providers*).

Figure 1 presents a graphical representation of a simple system drawn using SOCIOPATH. Consider that a person `John` wants to achieve the activity "accessing the

1. The words in italic in this section refer to keywords in the SOCIOPATH meta-model

http://hal.archives-ouvertes.fr/hal-00725098

document `toto` using `GoogleDocs`". In the social world, the person `John` owns some `Data`, a `PC` and an `iPad`. `Microsoft`, `Google` and `Apple` are legal entities which provide resources and artifacts. `Renater`, `Orange` and `SFR` are French telecom companies. John's `iPad` is connected to `SFR Servers` and `Renater Servers` and John's `PC` is connected to `Orange Servers`. In the digital world, the operating system `Windows` is running on John's PC. `Windows` supports `IExplorer`. John's `iPad` supports the running `iOS`, which supports the application `Safari`. John's `data` are represented in the digital world by the document `toto` that is supported by the physical resources owned by Google. We consider `Google Cloud` as the storage system used by the application `GoogleDocs`. By applying the SOCIOPATH rules on this example, we obtain the relations of *access* and *control* shown in Figure 1 where Jonh has the following minimal paths to access `toto`:

$\widehat{\sigma}_1$ ={John, Windows, IExplorer, ADSL Network, Google Cloud, GoogleDocs, toto}.
$\widehat{\sigma}_2$ ={John, iOS, Safari, SFR Network, Google Cloud, GoogleDocs, toto}.
$\widehat{\sigma}_3$ ={John, iOS, Safari, Professional Network, Google Cloud, GoogleDocs, toto}.

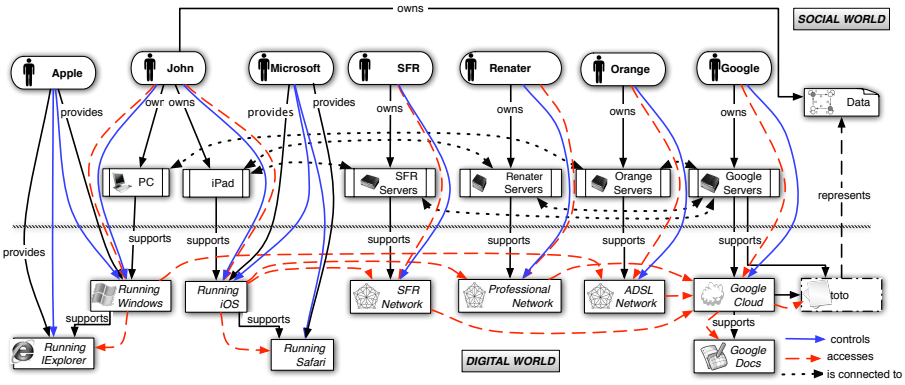


Fig. 1: Graphical representation of a system for the activity "John *accesses* a document `toto` on `GoogleDoc`" using SOCIOPATH

For simplicity sake, in the current paper we voluntary limit the digital activities to those that can be represented using a straight path. We do not consider activities that need multiple paths in parallel to be achieved. Most of the popular activities can be illustrated this way, such as connecting to a search engine, consulting a web page, publishing a picture, editing a document, *etc.* In the next sections, "accessing a document" is our illustrative activity.

3 Inferring the trust value of a system for an activity

In order to evaluate the trust level of a particular user in a system for a particular activity, we first obtain a coarse-grained view of the system, from a SOCIOPATH model, as a weighted directed acyclic graph (WDAG) (*cf.* Section 3.1). This graph represents

the system allowed to perform the digital activity of the user. We then apply a probabilistic approach on this graph (*cf.* Section 3.2) to calculate the trust level of a user in a system for an activity achieved through the different paths in the graph.

3.1 A SOCIOPATH model as a weighted directed acyclic graph

We simplify the representation of SOCIOPATH by using only *access* and *control* relations derived from SOCIOPATH rules. We combine an artifact, the set of persons controlling it and the set of physical resources supporting it into one unique component. These merged components are represented by the nodes in the WDAG. The edges in the WDAG represent the relations' *access*. A user performs an activity by passing through successive *access* relations of the graph, so-called a *path* [2]. A user who wants to achieve an activity associates each node with a trust value. To summarize, a system that enables a user to achieve an activity can be formally modeled as a tuple:
$\alpha_{\omega,P} =< \mathbb{N}_\omega, \mathbb{A}_\omega, t_\omega >$ where:

- P: the user who wants to achieve an activity.
- ω: the activity the user wants to achieve.
- $\mathbb{N}_\omega$: the set of nodes in a system for an activity. Each node aggregates one artifact, the persons who control it and the physical resources that support it.
- $\mathbb{A}_\omega \in \mathbb{N}_\omega \times \mathbb{N}_\omega$: the set of edges in a system. From the rules of SOCIOPATH and the aggregation we made for a node, our WDAG exhibits only the relation *access*.
- $t_\omega : \mathbb{N} \rightarrow [0, 1]$: a function that assigns to each node a trust level, which we assume to be within the interval [0,1], where 0 means not trustworthy at all and 1 means fully trustworthy. The evaluation of these values differs from one person to another. There are several ways to construct this trust level. We can figure out different objective and subjective factors that impact this trust level like the reputation of the persons who control the artifact, their skills, the performance of the physical resource that supports the artifact or the personal experience with this artifact. We thus have $t_\omega(N) = f(t^F_\omega, t^{\mathcal{P}}_\omega, t^{\mathcal{PR}}_\omega)$, where t^F_ω, $t^{\mathcal{P}}_\omega$, $t^{\mathcal{PR}}_\omega$ are the trust value assigned to an artifact F, the set of persons $\mathcal{P}$ who control F, the set of physical resources $\mathcal{PR}$ which support F respectively for a given activity ω. The meaning of the resulting trust value in a node depends on the employed function f to compute this value [8]. For instance, if Bayesian inference is employed to evaluate it as is done in [9], the node trust value is considered as *the probability by which a user believes that a node can perform an expected action for a given activity* [10]. However, in this work, we do not address the issue of computing this value. Moreover, in this study, we suppose that the edges are trustworthy, and we do not assign a level of trust to the edges.

Figure 2 shows the system presented in Figure 1 as a merged WDAG where each node represents an artifact with all additional information as physical resources it depends on and persons who control it, and each edge represents the relation *accesses*. The associated value on the node represents the level of John's trust in this node. The paths that enable John to access toto become: σ_1 ={`A, C, E, H, I`}; σ_2 ={`A, C, F, H, I`}; σ_3 ={`B, D, G, H, I`}.

2. If there is no ambiguity, we denote a minimal path through the WDAG by simply a path σ.

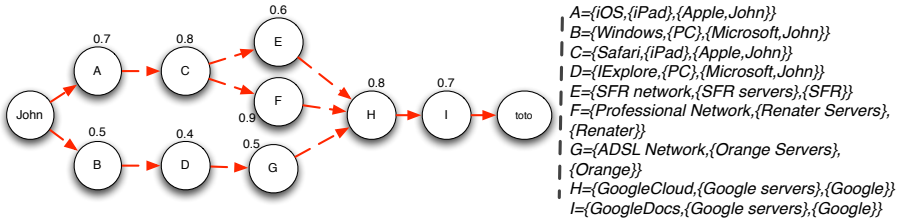


Fig. 2: The activity "John accesses a document `toto` on `GoogleDoc`" as a WDAG

3.2 SocioTrust: A probabilistic approach to infer the system trust value

Gambetta in [10] argues that: *When we say we trust someone or that someone is trustworthy, we implicitly mean that the probability that he will perform an action that is beneficial or at least not detrimental to us is high enough for us to consider engaging in some form of cooperation with him.* According to this argument, we can consider the trust value as the probability, by which one party believes that another party can perform an expected action in a certain situation [4].

We consider thus the following (Table 1 summarizes the notations used here).

- **Trust in a node**: The trust value of a user P in a node N for an activity ω is the probability, by which P believes that N provides her the expected services for ω. Then, we have $t(N) = \mathbf{P}(\lambda^N)$.
- **Trust in a path**: The trust value of a user P in a path σ for an activity ω is the probability, by which P believes that σ enables her to achieve ω. Then, we have $t(\sigma) = \mathbf{P}(\lambda^\sigma)$.
- **Trust in a system**: The trust value of a user P in a system α for an activity ω is the probability, by which P believes that α enables her to achieve ω. Then, we have $t(\alpha) = \mathbf{P}(\lambda^\alpha)$.

We consider trust in a node, a path or a system as a value of probability. Hence, probability theory is the used tool to obtain the formula of these probabilities, as we show in the next section [11].

3.2.1 Trust in a path (formal evaluation):

The trust level of a person in a path for an activity is the probability that all the nodes that belong to this path provide the expected services for the activity. Let $\sigma = \{N_1, N_2, \ldots, N_n\}$ be a path that enables a person P to achieve an activity ω. The trust level of a person P to achieve an activity through $\sigma = \{N_1, N_2, \ldots, N_n\}$ is the probability that all the nodes $\{N_i\}_{i\in[1..n]}$ provide the expected services for the activity. Thus $\mathbf{P}(\lambda^\sigma)$ is computed as follows:

$$\mathbf{P}(\lambda^\sigma) = \mathbf{P}(\lambda^{N_1} \wedge \lambda^{N_2} \wedge \ldots \wedge \lambda^{N_n})$$

The event λ^{N_i} means that N_i provides the expected services for an activity. Since the graph is acyclic, then the nodes $N_1, \ldots, N_n$ are different in the path, thus each λ^{N_i} is independent from all others. Hence, we can rewrite the trust in a path as follows:

$$\mathbf{P}(\lambda^\sigma) = \mathbf{P}(\lambda^{N_1}) \times \mathbf{P}(\lambda^{N_2}) \times \ldots \times \mathbf{P}(\lambda^{N_n}) = \prod_{i=1}^{n} \mathbf{P}(\lambda^{N_i}) \quad (1)$$

Concept	*Notation*	Concept	*Notation*	Concept	*Notation*
an activity	ω	a user who wants to achieve an activity	P	the probability of an event	$\mathbf{P}(\lambda)$
a node	N	a path	σ	a system	α
trust in a node value for an activity	$t(N)$	trust in a path value for an activity	$t(\sigma)$	trust in a system value for an activity	$t(\alpha)$
the event "N provides the expected services for an activity"	λ^N	the event "P achieves an activity through the path σ"	λ^σ	the event "P achieves an activity through the system"	λ^α
For a given activity ω achieved by a person P, the symbols ω, P are omitted for simplicity if there is no ambiguity					

Table 1: List of symbols and notations

3.2.2 Trust in a system (formal evaluation): The trust level of a person P in a system α to achieve an activity is the probability that she achieves her activity through one of the paths in the system. To evaluate the trust in a system for an activity, two cases have to be considered: (1) the paths are independent *i.e.,* they have no nodes in common and (2) the paths are dependent *i.e.,* there exists at least one node in common. The following shows how we use probability theory for these two cases.

1. **Independent paths:**
   Let $\{\sigma_i\}_{i\in[1..m]}$ be independent paths that enable a person P to achieve an activity. The probability of achieving the activity through a system, $\mathbf{P}(\lambda^\alpha)$, is the probability of achieving the activity through one of the paths σ_i. Thus $\mathbf{P}(\lambda^\alpha)$ is computed as follows:
   $$\mathbf{P}(\lambda^\alpha) = \mathbf{P}(\lambda^{\sigma_1} \vee \lambda^{\sigma_2} \vee \ldots \vee \lambda^{\sigma_m})$$
   Since the paths are independent then the equation can be rewritten as follows:
   $$\mathbf{P}(\lambda^\alpha) = 1 - \prod_{i=1}^{m}(1 - \mathbf{P}(\lambda^{\sigma_i}))$$
   For instance, if a person has two independent paths to achieve an activity then:
   $$\begin{aligned}\mathbf{P}(\lambda^\alpha) &= \mathbf{P}(\lambda^{\sigma_1} \vee \lambda^{\sigma_2}) = 1 - (1 - \mathbf{P}(\lambda^{\sigma_1})) \times (1 - \mathbf{P}(\lambda^{\sigma_2})) \\ &= \mathbf{P}(\lambda^{\sigma_1}) + \mathbf{P}(\lambda^{\sigma_2}) - \mathbf{P}(\lambda^{\sigma_1}) \times \mathbf{P}(\lambda^{\sigma_2})\end{aligned} \tag{2}$$
2. **Dependent paths:** To evaluate the trust through dependent paths, we begin from a simple case where a system has two paths before generalizing.
   2.1. ***Two dependent paths with one common node:*** Let σ_1, σ_2, be two paths that enable a person P to achieve an activity. $\sigma_1 = \{N, N_{1,2}, \ldots, N_{1,n}\}$, $\sigma_2 = \{N, N_{2,2}, \ldots, N_{2,m}\}$. These two paths have a common node, which is N and so they are dependent. Thus the probability that a person P achieves the activity ω through the system α is computed as follows:
   $$\mathbf{P}(\lambda^\alpha) = \mathbf{P}(\lambda^{\sigma_1} \vee \lambda^{\sigma_2}) = \mathbf{P}(\lambda^{\sigma_1}) + \mathbf{P}(\lambda^{\sigma_2}) - \mathbf{P}(\lambda^{\sigma_1} \wedge \lambda^{\sigma_2})$$
   The probability $\mathbf{P}(\lambda^{\sigma_1} \wedge \lambda^{\sigma_2})$ can be rewritten using conditional probability as the two paths are dependent.
   $$\begin{aligned}\mathbf{P}(\lambda^\alpha) &= \mathbf{P}(\lambda^{\sigma_1}) + \mathbf{P}(\lambda^{\sigma_2}) - \mathbf{P}(\lambda^{\sigma_2}) \times \mathbf{P}(\lambda^{\sigma_1}|\lambda^{\sigma_2}) \\ &= \mathbf{P}(\lambda^{\sigma_1}) + \mathbf{P}(\lambda^{\sigma_2}) \times (1 - \mathbf{P}(\lambda^{\sigma_1}|\lambda^{\sigma_2}))\end{aligned}$$
   We have to compute $\mathbf{P}(\lambda^{\sigma_1}|\lambda^{\sigma_2})$ which is the probability that P achieves the activity through σ_1 once it is already known that P achieves the activity

through σ_2. Thus it is the probability that N, $\{N_{1,i}\}_{i\in[1..n]}$ provide the expected services for this activity, once it is known that N, $\{N_{2,i}\}_{i\in[1..m]}$ provided the expected services. Thus N has already provided the expected services. Hence, $\mathbf{P}(\lambda^{\sigma_1}|\lambda^{\sigma_2}) = \prod_{i=2}^{n}\mathbf{P}(\lambda^{N_{1,i}})$, where $\lambda^{N_{1,i}}$ is the event "$N_{1,i}$ provides the necessary services for the activity".

$$\begin{aligned}\mathbf{P}(\lambda^{\alpha}) &= \mathbf{P}(\lambda^{N}) \times \prod_{i=2}^{n}\mathbf{P}(\lambda^{N_{1,i}}) + \mathbf{P}(\lambda^{N}) \times \prod_{i=2}^{m}\mathbf{P}(\lambda^{N_{2,i}}) \times (1 - \prod_{i=2}^{n}\mathbf{P}(\lambda^{N_{1,i}})) \\ &= \mathbf{P}(\lambda^{N}) \times \left[\prod_{i=2}^{n}\mathbf{P}(\lambda^{N_{1,i}}) + \prod_{i=2}^{m}\mathbf{P}(\lambda^{N_{2,i}}) \times (1 - \prod_{i=2}^{n}\mathbf{P}(\lambda^{N_{1,i}}))\right] \\ &= \mathbf{P}(\lambda^{N}) \times \left[\prod_{i=2}^{n}\mathbf{P}(\lambda^{N_{1,i}}) + \prod_{i=2}^{m}\mathbf{P}(\lambda^{N_{2,i}}) - \prod_{i=2}^{m}\mathbf{P}(\lambda^{N_{2,i}}) \times \prod_{i=2}^{n}\mathbf{P}(\lambda^{N_{1,i}})\right]\end{aligned}$$

From Equation 2 we can note that the term:

$$\prod_{i=2}^{n}\mathbf{P}(\lambda^{N_{1,i}}) + \prod_{i=2}^{m}\mathbf{P}(\lambda^{N_{2,i}}) - \prod_{i=2}^{m}\mathbf{P}(\lambda^{N_{2,i}}) \times \prod_{i=2}^{n}\mathbf{P}(\lambda^{N_{1,i}})$$

is the probability that P achieves the activity through $\sigma_1' = \{N_{1,2}, \ldots, N_{1,n}\}$ or $\sigma_2' = \{N_{2,2}, \ldots, N_{2,m}\}$ which are the paths after eliminating the common nodes. Thus the previous equation can be rewritten as follows:

$$\mathbf{P}(\lambda^{\alpha}) = \mathbf{P}(\lambda^{N}) \times \mathbf{P}(\lambda^{\sigma_1'} \vee \lambda^{\sigma_2'})$$

2.2. ***Two dependent paths with several common nodes:*** Let σ_1, σ_2, be two paths that enable a person P to achieve an activity. These two paths have several common nodes. By following the same logic as in 2.1., we compute the probability that a person P achieves activity ω through system α as follows:

$$\mathbf{P}(\lambda^{\alpha}) = \prod_{N\in\sigma_1\cap\sigma_2} \mathbf{P}(\lambda^{N}) \times \mathbf{P}(\lambda^{\sigma_1'} \vee \lambda^{\sigma_2'}) : \sigma_1' = \sigma_1 \setminus \sigma_2, \sigma_2' = \sigma_2 \setminus \sigma_1.$$

2.3. ***Several dependent paths:*** A person may have several paths l with common nodes.

$$\mathbf{P}(\lambda^{\alpha}) = \mathbf{P}(\lambda^{\sigma_1} \vee \lambda^{\sigma_2} \vee \ldots \vee \lambda^{\sigma_l}) =$$

$$\mathbf{P}(\lambda^{\sigma_1} \vee \lambda^{\sigma_2} \vee \ldots \vee \lambda^{\sigma_{l-1}}) + \mathbf{P}(\lambda^{\sigma_l}) - \mathbf{P}(\lambda^{\sigma_l}) \times \mathbf{P}(\lambda^{\sigma_1} \vee \lambda^{\sigma_2} \vee \ldots \vee \lambda^{\sigma_{l-1}}|\lambda^{\sigma_l}) \quad (3)$$

Let us discuss these terms one by one:

- $\mathbf{P}(\lambda^{\sigma_l})$ can be computed directly from Equation 1.
- $\mathbf{P}(\lambda^{\sigma_1} \vee \lambda^{\sigma_2} \vee \ldots \vee \lambda^{\sigma_{l-1}})$ can be computed recursively using Equation 3.
- $\mathbf{P}(\lambda^{\sigma_1} \vee \lambda^{\sigma_2} \vee \ldots \vee \lambda^{\sigma_{l-1}}|\lambda^{\sigma_l})$ needs first to be simplified. If we follow the same logic we discussed in Section (2.1.), the term $\mathbf{P}(\lambda^{\sigma_1} \vee \lambda^{\sigma_2} \vee \ldots \vee \lambda^{\sigma_{l-1}}|\lambda^{\sigma_l})$ can be replaced by the term $\mathbf{P}(\lambda^{\sigma_1'} \vee \lambda^{\sigma_2'} \vee \ldots \vee \lambda^{\sigma_{l-1}'})$ where we obtain each $\lambda^{\sigma_i'}$ by eliminating the nodes in common with σ_l.
- $\mathbf{P}(\lambda^{\sigma_1'} \vee \lambda^{\sigma_2'} \vee \ldots \vee \lambda^{\sigma_{l-1}'})$ can be computed recursively using Equation 3, and recursion is guaranteed to terminate when the number of paths is finite.

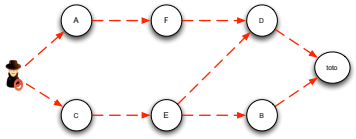
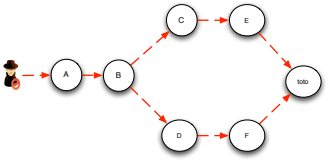
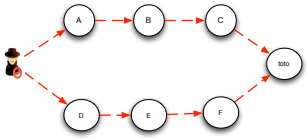
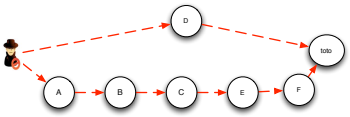
α		$t_\omega(\alpha)$	α		$t_\omega(\alpha)$
α_1		0.4409	α_2		0.0144
α_3		0.507	α_4		0.9003

Table 2: Different systems and their trust value

4 Experimental evaluations

This section presents different experiments, their results, analysis and interpretation. The main objectives are *(i)* to study the influence of the system organization on the trust values, and *(ii)* to confront this approach with real users. The first two experiments are related to the first objective while the third experiment is devoted to the second.

4.1 Influence of the system architecture on the trust value

SocioTrust is motivated by the hypothesis that studying trust in the separate nodes that construct a system does not give an accurate picture of the trustworthiness of the system as a whole. To validate this hypothesis, we apply our equations on different systems that have the same number of nodes `A,B,C,D,E,F` and the same values of trust assigned to each node, but assembled in different topologies as presented in Table 2. The values of trust associated to nodes `A,B,C,D,E,F` are $0.1, 0.2, 0.3, 0.9, 0.8, 0.7$ respectively. We calculate the trust value $t_\omega(\alpha)$ of each system. We obtain very divergent results varying from 0.0144 to 0.9003 as illustrated in Table 2. Collecting the values of trust in each separated node in a system is not enough to determine if the system is trustworthy or not for an activity. One must also know how the system is organized. For example, in α_2, all the paths contain the nodes `A` and `B` and the trust values in these nodes is quite low, 0.1 and 0.2 respectively, so the system trust value is also low due to the strong dependency on these two nodes.

4.2 Influence of the path length and the number of paths on the trust value

We conducted several simulations to observe the evolution of the trust value for an activity according to some characteristics in the graph. As a dataset, we considered random graphs composed of 20 to 100 nodes, and of 1 to 15 paths. Each node in the graph is associated with a random value of trust from a predefined range.

Firstly, the evolution of trust values according to the path lengths in a graph is evaluated. Each simulated graph is composed of 5 paths with lengths varying from 1 to 15 nodes. Different ranges of trust values towards the nodes were simulated, namely:

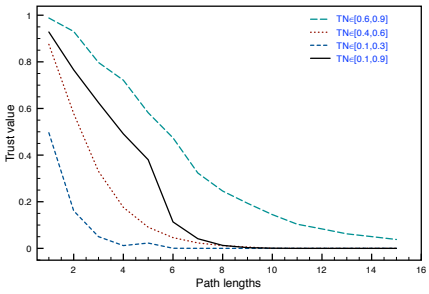


Fig. 3: System trust value according to the length of paths

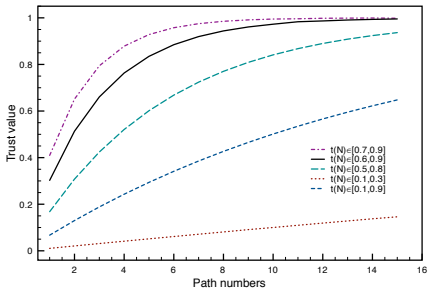


Fig. 4: System trust value according to the number of paths

$[0.1, 0.4]$, $[0.4, 0.6]$, $[0.6, 0.9]$ and $[0.1, 0.9]$. Figure 3 illustrates the impact of the path lengths on the trust value. Note that, the system trust value decreases when the length of paths increases. This reflects the natural intuition that the measure of trust in a path falls as the path gets longer, which is coherent with most of the existing results [12,13,14].

Secondly, we set the path lengths to 5 nodes and we increased the number of paths from 1 up to 15 in order to observe the variation of the trust values. Again, different node trust values were simulated: $[0.1, 0.3]$, $[0.5, 0.8]$, $[0.6, 0.9]$, $[0.7, 0.9]$ and $[0.1, 0.9]$. Simulation results are reported in Figure 4 which show that the trust value increases as the number of paths increase. This reflects the intuition that the measure of trust in a system for an activity rises when the number of ways to achieve this activity increases.

4.3 Social evaluation: a real case

In order to evaluate SOCIOTRUST in a real use case, we modeled a subpart of the LINA research laboratory system[3] using SOCIOPATH. We applied the rules of SOCIOPATH on this system for the activity "a user accesses a document toto that is stored on the SVN server at LINA". Due to space constraints and privacy issues, Figure 5 presents only the WDAG of LINA for this activity, with anonymous nodes. We recall that each node represents a software that is controlled by persons and supported by physical resources. For the sake of clarity, we simplify the underlying graph as much as possible. Based on this context, we conducted an opinion survey among twenty members of LINA including, PhD students, professors and computer technicians about their level of trust in each node. The survey allows to infer values of function f *(cf. Section 3.1)* given by real users. For each person, we have computed the system trust value according to the methodology presented in Section 3. Table 3 presents The survey data and the computed trust value in the system according to LINA members. Over a second phase, we asked each user for feedback about the system trust values computed with respect to their level of trust in the nodes. The last column of Table 3 shows this feedback, where ✓ means that they are satisfied with the value, and $\times$ means that they are not satisfied. 75% of the users are satisfied with the computation. Unsatisfied users argue that they expect a higher trust value. The node trust values of the unsatisfied users,

3. https://www.lina.univ-nantes.fr/

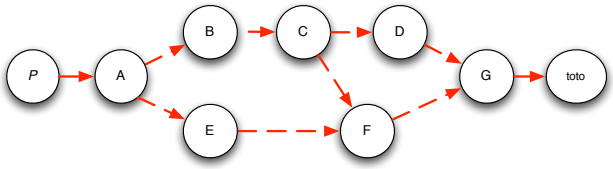


Fig. 5: LINA's WDAG for the activity "accessing a document toto on the SVN"

	A	B	C	D	E	F	G	System trust value	User's feedback about the system trust value
P_1	0.5	0.5	1	0.5	0.5	1	1	0.4375	✓
P_2	0.7	1	1	0.7	0.7	1	1	0.847	✓
P_3	0.5	0.5	1	0.7	0.5	1	1	0.4375	×
P_4	0.6	0.6	0.8	0.7	0.6	0.8	0.6	0.3072	×
P_5	0.8	0.8	1	0.8	0.8	1	0.9	0.8202	✓
P_6	0.9	0.9	1	0.9	0.9	0.9	0.9	0.9043	✓
P_7	0.6	0.6	0.7	0.6	0.6	0.6	0.7	0.2770	×
P_8	0.8	0.6	1	0.9	0.8	0.8	1	0.7416	✓
P_9	0.7	0.5	1	0.4	0.7	0.6	0.9	0.4407	✓
P_{10}	0.8	1	0.7	0.8	0.8	0.9	0.8	0.6975	✓
P_{11}	0.5	0.5	0.9	0.5	0.5	0.5	0.9	0.2473	×
P_{12}	0.95	0.95	0.8	0.8	0.95	0.95	0.8	0.8655	✓
P_{13}	0.8	0.9	0.8	0.7	0.95	0.8	0.7	0.6433	✓
P_{14}	0.8	0.7	0.9	0.7	0.9	0.8	0.8	0.6652	✓
P_{15}	0.9	0.8	0.8	0.9	0.9	0.9	0.8	0.7733	✓
P_{16}	0.7	0.6	0.6	0.6	0.8	0.7	0.6	0.337	✓
P_{17}	0.5	0.9	0.8	0.7	0.9	0.5	0.8	0.3807	×
P_{18}	0.7	0.7	1	0.7	0.6	0.7	1	0.6088	✓
P_{19}	0.8	0.8	1	1	1	0.8	1	0.8704	✓
P_{20}	0.9	0.9	0.8	0.9	0.9	0.9	0.8	0.7971	✓

Table 3: User's trust value in the system SVN in LINA

have relatively low values (around 0.5 or 0.6) compared to the other users. These users explain that the lack of knowledge about some nodes leads them to vote with a neutral value (0.5 or 0.6) which for them considered neither trustworthy, nor untrustworthy. Clearly, such behavior is not compatible with a probabilistic interpretation where 0.5 is no more *neutral* than any other possible value. The explanations provided by users reveal an interesting point; even in the case of a local environment and even considering advanced users, not everyone is in possession of all the information necessary for an informed assessment. To conform to this reality and model this phenomenon, it requires to use a formalism allowing to express uncertainty related to incompleteness of available information. Classical probability theory is limited in expressing ignorance or uncertainty while subjective logic [15] was proposed to deal with this issue. In our future work we plan to extend SOCIOTRUST to use subjective logic.

5 Related Work

This paper proposes SOCIOTRUST, an approach to evaluate the system trust value for an activity as a combination of several trust values through a graph. This work is related to two domains: social networks and service-oriented computing (SOC).

Usually, a social network is represented as a graph where the nodes are persons and the edges reflect the relations between these persons. The values associated to the edges represent the value of trust between these persons. Trust propagation problem in

social network focuses on finding a trust value toward a defined person or resource through the multiple paths that relate the trustor with the trustee. A lot of metrics have been proposed to calculate this trust value like the one of Richardson et al. [16], the TidalTrust [14], the SUNNY algorithm [17], the work of Agudo *et al.* [18]. SOCIOTRUST converges with these works on some points like navigating on the graph between the source and the target to collect the values of trust and combining these values to obtain the general trust value but it diverges in other points like, the values of trust associated to each node in our work are values attributed by the source node which represent her trust in these nodes. In their works, the values associated to the edges represent the trust between the nodes related with this edge. Hence, these works discuss the problem of trust propagation through a graph, while SOCIOTRUST focuses on finding a trust value toward the whole graph that reflects an activity performed through it.

In SOC, a service invokes other services forming a composite service, so the composite service can be represented as a graph where the nodes represent the service components and the edges represent the relation of invocation. In [13,19,9], authors evaluate the trust toward the composite service by considering the value of trust as probability depending on the definition presented in [4]. They calculate a global trust value toward the separated services and they use the theory of probability to evaluate the global trust value of the composite services. These works are similar to our proposal in some points. Firstly, the value associated to a node in the graph is represents the value of trust toward a service. Secondly, they consider this value as a probability that the node performs a given action that enables a user to achieve her activity. However, they diverge from SOCIOTRUST in a main point. In their work, the computed trust value is toward a certain choice (path) of the composite services where in our work, it is toward the whole system including all the paths that enable a user to achieve an activity.

The trust evaluation proposed in these two domains cannot be straightly adopted in our work due to the difference in the graph nature between their works and ours.

6 Conclusion and Perspectives

In this paper, we present a new notion of trust: trust in a system for an activity. We propose SOCIOTRUST, a probabilistic approach to calculate the system trust value. We conduct some experiments to illustrate that the system construction is a key factor in evaluating the user trust value in a system. Finally, we confront our approach with real user opinions based on a real modeled system to extract the limitations of this proposition. A serious limitation of our study is that trust values have been considered as a traditional probability where expressing ignorance or uncertainty is not possible. Subjective logic which is an extension of probability theory can deal with this issue. We are currently extending SOCIOTRUST to use subjective logic.

References

1. Marsh, S.: Formalising Trust as a Computational Concept. PhD thesis, University of Stirling (1994)

2. Moyano, F., Fernández-Gago, M.C., Lopez, J.: A Conceptual Framework for Trust Models. In: Proceedings of the 9th international conference on Trust, Privacy and Security in Digital Business (TrustBus). (2012) 93–104
3. Viljanen, L.: Towards an Ontology of Trust. In: Proceedings of the 2nd international conference on Trust, Privacy, and Security in Digital Business (TrustBus). (2005) 175–184
4. Jøsang, A., Ismail, R., Boyd, C.: A Survey of Trust and Reputation Systems for Online Service Provision. Decision Support Systems **43**(2) (2007) 618–644
5. Zhang, P., Durresi, A., Barolli, L.: Survey of Trust Management on Various Networks. In: International Conference on Complex, Intelligent and Software Intensive Systems (CISIS'11). (2011) 219–226
6. Yan, Z., Holtmanns, S.: Trust Modeling and Management: from Social Trust to Digital Trust. In: Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions. (2007)
7. Alhadad, N., Lamarre, P., Busnel, Y., Serrano-Alvarado, P., Biazzini, M., Sibertin-Blanc, C.: SocioPath: Bridging the Gap between Digital and Social Worlds. In: 23rd International Conference on Database and Expert Systems Applications (DEXA). (2012) 497–505
8. Mcknight, D.H., Chervany, N.L.: The Meanings of Trust. Technical report, University of Minnesota, Carlson School of Management (1996)
9. Li, L., Wang, Y.: Subjective Trust Inference in Composite Services. In: 24th Conference on Artificial Intelligence (AAAI). (2010) 1377–1384
10. Gambetta, D.: Can We Trust Trust? In Gambetta, D., ed.: Trust: Making and Breaking Cooperative Relations. Department of Sociology, University of Oxford (2000) 213–237
11. Carminati, B., Ferrari, E., Morasca, S., Taibi, D.: A Probability-Based Approach to Modeling the Risk of Unauthorized Propagation of Information in on-Line Social Networks. In: ACM Conference on Data and Application Security and Privacy, (CODASPY). (2011) 51–62
12. Hang, C.W., Wang, Y., Singh, M.P.: Operators for Propagating Trust and their Evaluation in Social Networks. In: Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems (AAMAS). (2009) 1025–1032
13. Li, L., Wang, Y.: A Subjective Probability Based Deductive Approach to Global Trust Evaluation in Composite Services. In: IEEE International Conference on Web Services (ICWS). (2011) 604–611
14. Golbeck, J.A.: Computing and Applying Trust in Web-Based Social Networks. PhD thesis, University of Maryland, College Park, College Park, MD, USA (2005) AAI3178583.
15. Jøsang, A.: A Logic for Uncertain Probabilities. International Journal of Uncertainty Fuzziness and Knowledge-Based Systems. **9**(3) (2001) 279–311
16. Richardson, M., Agrawal, R., Domingos, P.: Trust Management for the Semantic Web. In: Proceedings of the 2nd International Semantic Web Conference (ISWC). (2003) 351–368
17. Kuter, U., Golbeck, J.: SUNNY: A New Algorithm for Trust Inference in Social Networks Using Probabilistic Confidence Models. In: Proceedings of the National Conference on Artificial Intelligence (AAAI). (2007) 1377–1382
18. Agudo, I., Fernandez-Gago, C., Lopez, J.: A Model for Trust Metrics Analysis. In: Proceedings of the 5th international conference on Trust, Privacy and Security in Digital Business (TrustBus). (2008) 28–37
19. Li, L., Wang, Y.: Trust Evaluation in Composite Services Selection and Discovery. In: IEEE International Conference on Services Computing. (2009) 482 –485