IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 5 December 2023, accepted 5 January 2024, date of publication 22 January 2024, date of current version 1 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3357079

RESEARCH ARTICLE

New Aggregators for Global Reputation on Bi-Lattice Based Trust Model

BAPTISTE BELTZER[1], **EMMANUEL CONCHON**[2], **AND SYLVAIN GIROUX**[1]

[1]Laboratoire Domus, Département d'informatique, Faculté des sciences, Université de Sherbrooke, Sherbrooke, QC J1K 2R1, Canada
[2]XLIM, UMR CNRS 7252, Faculté des Sciences et Techniques, Université de Limoges, 87060 Limoges Cedex, France

Corresponding author: Baptiste Beltzer (baptiste.beltzer@usherbrooke.ca)

This work was supported in part by Age Well Networks of Centres of Excellence (NCE), in part by Medteq, in part by Fondation Berthiaume-Du Tremblay, in part by Fondation Luc Maurice, in part by Vidéotron, and in part by Mitacs.

ABSTRACT Within large and growing human communities where interactions occur, trust is a key factor to consider. Computational trust models have then been widely studied since the 2000s targeting items ratings (e.g. in e-commerce) or M2M (e.g. in IoT network). Among these models , EigenTrust is today one of the most popular and studied ones . It provides a global reputation calculation and is efficient in distributed networks, but not fully satisfactory for human interactions. On the opposite, the Bi-lattice model is well suited for human networks interactions such as solidarity networks and/or human services exchange networks but is limited to local trust results. In this paper, we propose a new aggregator that extends the Bi-lattice model to enable a global reputation calculation. This new aggregator discovers the trust links from the member whose score is to be evaluated to every other members he is connected to on the trust network. It then computes the global reputation of this member based on these trust links. Furthermore, it enables a lightweight approach, as it is able to compute a global reputation based only on a partial knowledge of the trust network. Throughout the paper, the proposed aggregator is presented, evaluated and compared to Eigentrust to show its effectiveness.

INDEX TERMS Aggregator, Bi-lattice, confidence, distrust, global model, local model, reputation model, trust.

I. INTRODUCTION

Since the 2000's, virtual communities have expanded widely. The rise of web 2.0 and now 3.0 has placed individual actors at the heart of digital content creation. Within those large and growing communities, and in a globalized world, knowing who you can trust is becoming a crucial issue. Research on computational trust has therefore increased, and computational trust models have been proposed. Most of them are adapted to goods evaluation (e.g. in e-commerce) or M2M (Machine to Machine) , but few of them effectively target the evaluation of trust between humans [1] .

In this work, we focus on solidarity human networks with real life services exchanges. These exchanges are performed by people who can meet each other in real life to provide and receive services, collaborate or help each other for daily life activities . The evaluation of human behaviors is then essential in this context . In Quebec, the Accorderie is connecting for nearly 20 years its members to create a solidarity network. Members from the same locality can exchange services, on the basis of their know-how and availability, without any financial compensation as the base currency is time. However, one of the problems of scaling up is the issue of trust. Currently, trust between members is checked only once before entering the private solidarity network , but this method is not viable on larger and more public networks.

To address this issue, we base our work on one of the few trust models that focuses on human networks which is the Bi-lattice once. This trust model proposes a good representation of human trust by jointly integrating the concepts of trust and distrust to refine the representation of the strength of trust relationships [2]. In fact, the use of a pair (trust, distrust) makes it possible to represent new stats such as the absence of information or information conflicts. Thus, this model provides a solid basis to implement a computational trust in a network such as the Accorderie. However, most works only provides local trust results. One of its main limitation is that

The associate editor coordinating the review of this manuscript and approving it for publication was Asad Waqar Malik.

it does not allow the community to agree on a universal score for each member.

Indeed, although human trust is subject to personal feelings, prejudices, or interpretations subjective and local trust models appear to be good representatives, they are quickly limited in their capacity. For example, local models generally don't allow producing results from or to a new member. Global models solve part of the problem: from new members to others, by allowing the community to agree on the reputation of each member. Obviously, the other direction (from the community to the new member) remains an issue. Another property of local models is the possibility of clans emerging. In the context of a solidarity network, we believe that clan grouping is undesirable, because if one group becomes the majority, the other clans risk exclusion through ostracism. On the contrary, the global approach enables to highlight negatively-judged behaviors, and network members can then solve the inherent problem.

In the context of the Accorderie, and for human solidarity networks in general, we believe it is desirable to design a trust model which use would foster good behavior rather than pinpoint malicious actors. The Bi-lattice based model remains a solid basis for the evaluation of human behavior and will serve as a basis for our own work. In this paper, we focus on the aggregation phase of the Bi-lattice model and present a new operator that aggregate the evaluations related to a member to compute his global reputation. Moreover, the high configurability of our aggregator makes it extremely versatile, with three main parameters:

- the size of the subnetwork centered on the candidate we want to evaluate: to adjust the quantity of information to be aggregated (a very small subnetwork size enables very fast calculations, at the risk of lower reliability; and increasing this parameter tends to the result obtained by aggregating the whole network).
- the weighting of strongly-convinced people. By emphasizing this parameter, we can over- or undervalue strongly-convinced opinions ("I trust a lot" or "I distrust a lot") versus indecisive ones ("I do not know" or "I am mitigating").
- the weighting related to the distance from the candidate makes it possible to adjust the impact of members close to the candidate versus distant members.

The first parameter concerns the quantity of information to be aggregated in order to obtain reliable results with a lightweight approach, while preserving maximum accuracy. The second and third parameters are characteristics of the network to which our aggregator applies. Indeed, the Bi-lattice model justifies the quality of its results on the evaluation of only one dataset [3]. But not all human networks are identical, and their properties can evolve. So, the configurability of our aggregator makes it more general and therefore more adaptable to different networks. An extended discussion on the choice of parameters can be found in the proposed aggregator evaluation part.

In the remaining of the paper, we focus in part II on the notion of computational trust by presenting the trust concepts and different trust models . In part III, we recall the Bi-lattice based model (based on [2], [3], [4] [5]) that serves as a basis for our work . Then, in part IV, we present our new highly configurable aggregator for the Bi-lattice base model. The goal of this new aggregator is to take advantage of the good representativeness of the Bi-lattice based model by trying to add configurability and integrate the strengths of global reputation models. In part V, we propose to evaluate our new aggregator against benchmark results proposed by Eigen-Trust. We based this comparison on the use of the dataset from a couch-surfing application. We also present a performance evaluation to search for an optimal configuration. Finally, we conclude with important results from evaluations and we present some limitations and future works.

II. COMPUTATIONAL TRUST

In this section, we present the concepts of trust, from social trust to computational trust. We then present various existing models.

A. TRUST CONCEPTS

Since the 2000's, research on reputation models has increased. Web 2.0 has provided users with new possibilities for interaction, collaboration or data sharing. Trust and reputation computational models are used as tools to measure the trust within these virtual communities.

Computational trust is a relatively recent concept, drawing on social trust to produce trust management models based on simulations or algorithms [1]. But social trust is a vague notion. This field of research is mainly covered by the social sciences (management, marketing, psychology, sociology, etc.), and there is no unanimity on the definition of these concepts. However, they generally include the notions of socialization, cooperation and risk-taking. In his thesis on the recommender systems [6], C.A. Haydar presents the historical aspect from the social sciences and propose a synthesis of definitions. Social trust generally expresses the belief of a member (or a group) towards another, in the will to cooperate. In an analysis of several definitions [7], S. Castaldo lists many redundant keywords, such as: individual, behavior, future, expectation, or even trustworthiness or confidence …

Research on computational trust then draws on concepts of social trust to formalize trust models, mainly in a machine context. S. Ruohomaa and L. Kutvonen recall in their survey [1] that the nature of social trust is a complicated phenomenon and that it is not certain that models should perfectly mimic human behavior. Indeed, the vast majority of studies focus on a systemic approach to trust, where network members are computer devices adopting purely rational behaviors.

In the following, we base our trust concept definitions on those proposed by F. Azzedin in his thesis [8] (or in [9], [10]), adapting them to the human context. In this work, we consider that trust expresses the belief that a member will act as expected. Conversely, distrust expresses the risk that a member will not act as expected. Finally, the reputation of a member is an expectation of its behavior based on the community's opinions.

In addition, several surveys in recent years have formalized taxonomies of trust models [9], [11]. These taxonomies classify trust models according to different dimensions, such as the trust components used to evaluate trust, computational constraints (network distribution, trust propagation or aggregation), or information discovery and trust advertisement. One of the main consequences of computational constraints (trust propagation and aggregation), information discovery and advertisement, is to define the scope of the result: global or local.

- Global trust (or reputation) models generally require a maximum amount of information to provide an individual reputation score, regardless of who is requesting the information. It is a universal score assigned to each member of the network. The term "global" has two meanings. The first meaning is the universality of the result : the score of each member is universal and therefore does not depend on who requires the information. The second meaning relates to the source of raw data : it means that the result integrates all the information of the network. This second meaning is not usually explained in presentations of global confidence models. This is an important detail in our context, as the parameters of our aggregator allow us to obtain results considered as global by aggregating only a subnetwork.
- Local trust models are models where the trust value exists only from one member to another: from the requester to the candidate. Each member has a trust level hat depends on who is requesting it . There are two local trust approaches: simplest non-collective approach and more advanced collective approach.
  - First, we can consider a "simple" trust approach, which is the closest to the social definition and the most subjective approach . Members judge, apprehend or express their opinions towards the others. In terms of calculation, the trust that a member A places in a member B is simply formulated by an aggregation based on the interactions between A and B . This first approach of local trust model do not consider the propagation of trust by transitivity and quickly presents its limits (e.g. member A cannot have any information about B before interacting with B if there has not been any contact yet).
  - A second approach, the collective one, uses more information and allows evaluating the trust of a member by aggregating my opinion as well as the opinions of my "friends" and that of my friends' friends ..., by using the propagation of trust . The collective approach of local trust model allows establishing a trust link between members A and B who have no yet interacted, if there is at least a propagation path between A and B.

B. TRUST MODELS

On one hand, one of the most popular global trust model to date is EigenTrust [12]. It computes an eigenvector of a normalized trust matrix based on local votes. Eigentrust has been proposed in the context of file sharing to judge the reliability of resources in a BitTorrent network. One of its greatest assets is that it is efficient in distributed networks. However, EigenTrust suffers from a number of weaknesses, such as cold startup, the impact of normalization or the belief in the honest feedback.

Many models have been derived from EigenTrust to try to solve these issues. Some integrate the similarity to evaluate the reliability of feedback like SimiTrust [13] or EigenTrust++ [14]. Others integrate new trust factors such as contribution quantity or a context and/or quality factors like PeerTrust [15], [16] or CuboidTrust [17]. Others still improve the computational efficiency and the cold start with a dynamic pre-trusted peer set as in HonestPeer [18].

On the other hand, one of the first and simplest local collective trust model is MoleTrust [19]. This is a lightweight model that provides local trust results based on a subnetwork limited to a fixed horizon.

Another approach is the one based on Bi-lattice [2], by integrating two values of confidence: trust and distrust simultaneously. This approach allows a better interpretation of the results by integrating the representation of two new behaviors: ignorance and contradictory information. Moreover, the authors of the first papers on the Bi-lattice model propose some new operators to compute the propagation and the aggregation of trust and distrust values.

III. BI-LATTICE BASED MODEL OVERVIEW

The confidence management model based on Bi-lattice was first introduced in 2006 [2], its authors present a new model of confidence and introduce its values space,

$$\mathcal{BL} = [0, 1]^2. \tag{1}$$

They assume that trust and distrust can coexist. This space is used to represent the different opinions that a member can attribute to another: $(t, d) = (1, 0)$ for a total trust and $(t, d) = (0, 1)$ for a total distrust (and all these gradients). The values $(t, d) = (0, 0)$ and $(t, d) = (1, 1)$ allow representing respectively the ignorance and the conflict of information.

Moreover, this bivalent representation allows knowing the level of knowledge

$$\forall (t, d) \in \mathcal{BL}, \quad k = t + d, \quad \text{and } k \in [0, 2]. \tag{2}$$

The level of knowledge is an important tool to highlight three zones of confidence:

- $k < 1$ is the area of lack of knowledge.
- $k = 1$ is the line of perfect knowledge.
- $k > 1$ is the area of excess knowledge, therefore contradictory information.

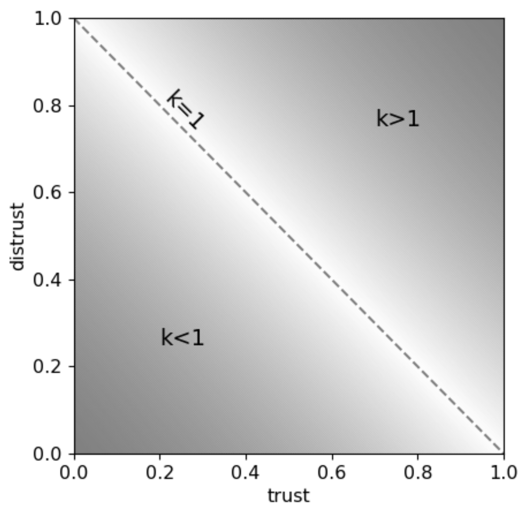


FIGURE 1. Representation of the knowledge levels.

We can represent these zones in a two-dimensional graph presented in Fig. 1.

A. PROPAGATION OPERATORS

Reference [2] present the problem of propagation, where: "if the opinion of member A in B is (t_{AB}, d_{AB}) and the opinion of member B in C is (t_{BC}, d_{BC}), what information can be derived about the opinion of member A in C ?" The propagation problem has been further developed in [4].

Formally, a propagation operator is an application $PR : \mathcal{BL}^2 \to \mathcal{BL}$. This operator is not necessarily commutative or associative. Here are different propagators among the main ones proposed:

- The first one exhibits a skeptical behavior like: "I only consider the opinions of members I trust".

$$PR_1((t_{AB}, d_{AB}), (t_{BC}, d_{BC})) = (t_{AB} \cdot t_{BC}, t_{AB} \cdot d_{BC}) \quad (3)$$

- The second one present a paranoid behavior: "If I don't know, I don't trust" .

$$PR_2((t_{AB}, d_{AB}), (t_{BC}, d_{BC})) = (t_{AB} \cdot t_{BC}, (1 - d_{AB}) \cdot d_{BC}) \quad (4)$$

- This operator exhibits a behavior in accordance with the maxim, "the enemy of my enemy is my friend".

$$\begin{aligned} &PR_3((t_{AB}, d_{AB}), (t_{BC}, d_{BC})) \\ &= (t_{AB} \cdot t_{BC} + d_{AB} \cdot d_{BC} - t_{AB} \cdot t_{BC} \cdot d_{AB} \cdot d_{BC}, \\ &\quad t_{AB} \cdot d_{BC} + d_{AB} \cdot t_{BC} - t_{AB} \cdot t_{BC} \cdot d_{AB} \cdot d_{BC}) \end{aligned} \quad (5)$$

Reference [4] show that PR_2 and PR_3 can be complementary, allowing to reflect different confidence behaviors. However, for the following, we choose to use only PR_3 because it respects the propagation of ignorance (i.e. $\forall (t, d) \in \mathcal{BL}, PR_3((0, 0), (t, d)) = PR_3((t, d), (0, 0)) = (0, 0)$).

Moreover, as these propagators allow computing chains of variable length, it will be relevant to keep the length of the propagation chain in the result. So we can continue our value space to $(t, d, p) \in \mathcal{BL} \times \mathbb{N}^*$ where p is the length of the propagation path ($p = 1$ in the case of a direct opinion). From here, a score level defined only by (t, d) will be implicitly either $p = 1$, or p useless for the further reasoning.

B. AGGREGATION OPERATORS

In addition to propagation, [3] and [5] also questioned the aggregation problem: "if the opinion of member A in C is (t_{AC}, d_{AC}) and the opinion of member B in C is (t_{BC}, d_{BC}), what information can be derived about the general opinion of members A and B in C ?"

Formally, an aggregator operator is an application $AG : (\mathcal{BL} \times \mathbb{N}^*)^n \to \mathcal{BL}$. This operator must be commutative, but not necessarily associative. Moreover, some issues due to non associativity (and non distributivity of PR on AG) are discussed in the next subsection on the algebraic structure of the confidence space. Where propagators can be inspired by the usual multiplication, aggregators cannot be built as simply from the usual addition. The main risk is to simply increase the level of knowledge and risk $t > 1$ or $d > 1$, or both. The main operator used to build aggregators is the average. To help the design of these aggregators, [3] propose some properties that should be respected:

- The first property of aggregators is that of bounds: if (t, d) is the aggregation result of $(t_i, d_i)_{i \in [\![1,n]\!]}$, we should have: $min(t_i) \leq t \leq max(t_i)$; $min(d_i) \leq d \leq max(d_i)$ and $min(k_i) \leq k \leq max(k_i)$. The area according to these properties is shaded on the Fig. 2.
- The aggregators should be monotonous: For the trust order $<_t$ (resp. distrust order $<_d$), if $(t_i, d_i) \leq (t'_i, d'_i)$, then $AG((t_1, d_1), \ldots (t_i, d_i), \ldots (t_n, d_n)) \leq AG((t_1, d_1), \ldots (t'_i, d'_i), \ldots (t_n, d_n))$.
- $(0, 0)$ is the neutral element for aggregators.
- If all aggregate scores are (t, d), then the result of the aggregation is (t, d).
- If the same number of opposite scores (ie. (t, d) and (d, t)) are aggregated, the result should highlight this inconsistency. For example, we can have:

$$AG(\underbrace{(1, 0), \ldots (1, 0)}_{n/2}, \underbrace{(0, 1), \ldots (0, 1)}_{n/2}) = (1, 1). \quad (6)$$

AV is the first simplest aggregator. It's a standard arithmetic average, eliminating zero trust values $(0, 0)$ from the calculation. However, this aggregator is very sensitive to near zero values (e.g. $(0.001, 0.001)$ has a strong impact).

To improve the aggregation based on the arithmetic average, [3] propose $KAAV_g$ as a smarter average than AV. It's a weighted average, where weights are powers of the data reliability. The g power is called the knowledge reward, and the data reliability is the distance from the data to the line $k = 1$. Note that AV is $KAAV_0$.

A second and more advanced aggregators' family is based on OWA operators. An OWA operator is an ordered weighted average. In aggregation of $(s_1, \ldots, s_n)$, where the score

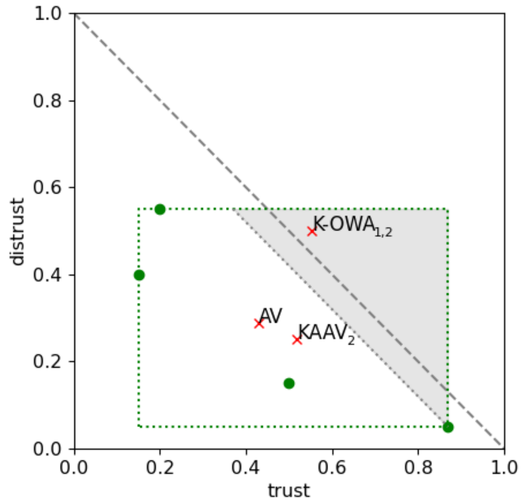


FIGURE 2. Example of some aggregation results (red crosses) from 4 arbitrary data (green dots). The shaded area is the area according to the properties of boundary.

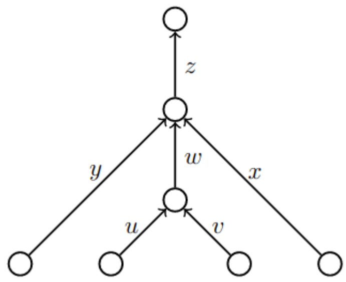


FIGURE 3. Example of some propagation and their final aggregation, where nodes are users and edges are direct opinion.

$s_i = (t_i, d_i)$, the OWA aggregators are defined by two OWA sub-operators:

$$OWA_{(<_t,v_t),(<_d,v_d)}(s_1, \ldots, s_n) = (OWA_{<_t,v_t}(t_1, \ldots, t_n), OWA_{<_d,v_d}(d_1, \ldots, d_n)). \quad (7)$$

where:

- $<_t$ (resp. $<_d$) is a total order on scores when calculating the trust (resp. distrust) part of the result.
- v_t (resp. v_d) is the associated weight vector for trust (resp. distrust) part .

$K - OWA_{a_t,a_d}$ Represent this family of aggregators. $<_t$ and $<_d$ are chosen as the standard order, and the two vectors of weights are generated from the parameters a_t and a_d.

The third family of aggregator is the path length dependent aggregators. $P - WA_\alpha$ is a path length dependent weighted average. Score weights are built according to the length of the aggregation path to reduce the impact of long paths. Another example of path length dependent aggregator is $P - IOWA_{a_t,a_d}$. It's similar to $K - OWA_{a_t,a_d}$ but the order is first induced by the path length and then by the trust (resp. distrust) values.

Finally, [5] introduce a last aggregator regrouping the advantages of OWA and path length dependent operators. $KP - OWA$ is the last proposed operator. It applies a double weighted average, firstly like $K - OWA$ and secondly like $P - WA$.

C. $\mathcal{BL}$ ALGEBRAIC STRUCTURE

One of the computational difficulties in the Bi-lattice based model is due to the weakness of its algebraic structure. Indeed, PR and AG are generally non-associative, and PR is generally non-distributive on AG. This observation requires overcoming situations such as:

- for $x, y, z \in \mathcal{BL}$, $PR(x, PR(y, z))$ is generally different of $PR(PR(x, y), z)$.
- for $x, y, z \in \mathcal{BL}$, $AG(x, AG(y, z))$ is generally different of $AG(AG(x, y), z)$.
- for $x, y, z \in \mathcal{BL}$, $PR(x, AG(y, z))$ is generally different of $AG(PR(x, y), PR(x, z))$.

To avoid these situations, it's necessary to adopt some convention:

- Due to the non-associativity of the propagation operators, it is necessary to define a generalization for the chains of propagation (if A has an opinion x on B who has an opinion y on C who has an opinion z on D). Reference [3] shows the advantages to perform the propagation in a right-to-left direction (notably, when there is no centralized database of all direct opinions): for $x, y, z \in \mathcal{BL}$, $PR(x, y, z) = PR(x, PR(y, z))$.
- Because of the non-associativity of the aggregation operators, and because these operators are not necessary binary, it is proposed to not compose this aggregator with itself but rather to aggregate a list of scores: for $x, y, z \in \mathcal{BL}$, $AG(x, AG(y, z)) = AG([x, y, z])$.
- Due to the non-distributivity of PR over AG, we can imagine that we start by computing all the propagation chains, and finally proceed to a final aggregation. So, only one final aggregation is calculated. Example: To compute the result present in Fig. 3, we compute $AG([PR(y, z), PR(u, w, z), PR(v, w, z), PR(x, z)])$. So after the aggregation operation, we can not perform any more calculations. The image space of the aggregator is then reduced to $\mathcal{BL}$. The length of the propagation does not generally have any more sense after an aggregation because the aggregation can incorporate different length paths.

D. NOTE ON THE OWA OPERATORS

Reference [3] and [5] show that the aggregators based on OWA operators are the most efficient. This result is experimentally justified by the capacity of the propagator/aggregator couple to retrieve a value voluntarily removed from the dataset. Two directly linked members A and B are selected, and the opinion (t_{AB}, d_{AB}) is deleted and taken as reference score. It is then tried to recompute (t'_{AB}, d'_{AB}) using the remaining indirect paths from A to B. Finally, on many trials, statistics measure the differences between the reference values (t, d) and the reconstructed values (t', d').

However, a fundamental point remains to be clarified: the construction of the weight vector for the application of the OWA operators. In the following, we present the original definition proposed for the weight vector, and then we propose another more modular construction adapted to the use of global aggregation.

IV. A NEW OPERATOR FOR GLOBAL AGGREGATION

In this section, we focus on the expected property of a global reputation model compared to a local model. We then present a new way to use aggregators to achieve global results. The focus is mainly on the role of the weight vector when using OWA-based aggregators.

A. LOCAL VS GLOBAL AGGREGATION

Global reputation models allow the emergence of a reputation score for each individual, independently of who emits the request. Furthermore, most global models also incorporate another notion of globality: all the information available in the network is used to compute individual reputations. In the following, we choose to use the term of quasi-global to consider an operator that respects the first property but not necessarily the second. A quasi-global aggregation allows generating for each member an individual reputation score independently of the requester, but that does not necessarily integrate all the data of the network.

In a cooperative local trust computation approach, we consider who emits the request. The principle is to aggregate the set of scores from A to B, where A is the requester and B is the candidate. Each score comes from a propagation chain of length p, where $p \in [\![1, h]\!]$, where h is the search horizon. This approach has several defects:

- First, if the length of the shortest path from A to B is greater than h, then this calculation does not give any results.
- Moreover, this technique, when it gives usable results, tends to favor clan groupings. Indeed, if A and B belong respectively to two subgroups G_1 and G_2, that each subgroup is strongly connected with score values globally "trusting", and that the intergroup links are rare and globally "distrusting", then the local trust calculation will make emerge a distrust from A to B. Thus, this tool does not show that B is globally trusted within his subgroup.
- Finally, if the members of the network have on average δ opinions about their neighbors, (i.e., $\delta = |E|/|V|$ in graph $G(V, E)$), then the exploration of the subnetwork of A bounded by a horizon h represents the exploration of $O(\delta^h)$ paths, of which only a fraction arrive to B. That is, only a fraction of the recovered information can be used in the aggregation calculation.

B. GENERAL IDEA

We propose to use a variant of $KP - OWA$ operator and perform a quasi-global aggregation to allow answering these three problems. The general idea is to aggregate the set of paths of length $p \in [\![1, h]\!]$ arriving at the candidate B (no matter where they come from), excluding paths with loop. Moreover, it is enough that an opinion is expressed towards B for the computation to give a result (although this result is not fully relevant if too little information is aggregated).

Finally, since the search for the paths leading to B is equivalent to the search for the paths from A to B, we show in the following part that there is a limit of the number of aggregated paths , beyond which, in depth research brings very little additional information.

To realize this aggregation centered on the candidate B, we chose to apply a variant of the most reliable aggregator presented in [5]. Indeed, we must reconsider the search horizon in terms of the desired computational efficiency. For a given horizon h, we will aggregate about δ^h paths. But how to define h ? Moreover, the choice of h does not provide information about a precise bound of the number of aggregated paths as long as we do not know the topology of the subnet of candidate B. Our approach proposes to define an integer γ of significant paths that we wish to aggregate (i.e., the number of paths that we consider both necessary and sufficient to appreciate the results). We then deduce h by a width search. This bound γ can be translated into a zero setting of the set of weight values w_i of the aggregation weight vector for all $i > \gamma$. γ is a personal parameter chosen by the requester. There is no "good" value for this parameter. Finally, it may be relevant to perform several calculations with different values of γ to get information about the subnetwork close to the candidate, as to observe clan groupings.

C. OWA WEIGHT VECTORS CONSTRUCTION

Usually, the OWA operator uses a vector of fixed weight as in [3] and [5]:

$$w_i = max\left(0, \left\lceil \frac{n}{\alpha} \right\rceil - i\right). \tag{8}$$

The vector is then normalized such that $\sum w_i = 1$. An important feature of this definition is that the vector has exactly $\lceil \frac{n}{\alpha} \rceil$ non-zero weight. So there will be $\lceil \frac{n}{\alpha} \rceil$ regarded score in the aggregation. Also note that w is also the definition of a decreasing arithmetic sequence bounded at 0.

This vector is an arbitrary choice and is not very configurable. In order to refine our results with respect to reference reputation algorithms, we choose to redefine this vector with more modularity. In this regard, we choose to use an arithmetic-geometric sequence. Moreover, for ease of use, we set $w_0 = 1$ representing the maximum weight (before normalization) and apply the bound γ to set the desired non-zero weight of w. So we have:

- $w_0 = 1$
- $\forall k \in [\![1, \gamma]\!], w_k = aw_{k-1} + b$
- $\forall k \in [\![\gamma, n]\!], w_k = 0$

On $[\![0, \gamma]\!]$, w is an arithmetic-geometric sequence define by $w_i = r - a^i r$, where $r = \frac{b}{1-a}$.

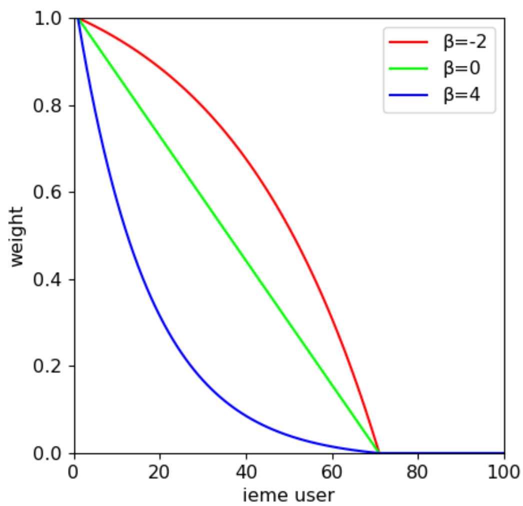


FIGURE 4. **Representation of the weights of a vector of size 100 with the $\gamma = 70$ bound for three β values.**

We also define a parameter $\beta \in [-\infty, \gamma]$ resulting from a and b to represent the proportions of decrease associated to the geometric part ($\beta = 0$ then represents an arithmetical sequence only). Then, we propose:

$$\begin{cases} a = 1 \text{ and } b = \dfrac{-1}{\gamma} & \text{if } \beta = 0 \\ a = 1 - \dfrac{\beta}{\gamma} \text{ and } b = a^{\gamma}\dfrac{a-1}{1-a^{\gamma}} & \text{else.} \end{cases} \quad (9)$$

So, we have:

$$w_i = \begin{cases} max\,(0, 1-b) & \text{if } \beta = 0 \\ max(0, a^i + b\dfrac{a^i - 1}{a-1}) & \text{else.} \end{cases} \quad (10)$$

The vector obtained from (10) is finally normalized.

With this definition, we can have different configurations of the weight vector (as shown in Fig. 4):

- $\beta < 0$, to minimize the difference in weight between the most relevant scores
- $\beta = 0$, to equalize the difference between the scores
- $\beta > 0$, to minimize the difference in weight between less relevant scores

D. PATH LENGTH DEPENDENT WEIGHT VECTORS CONSTRUCTION

Reference [5] present two constructions of the path length dependent weight vector: non-starred option and starred option. The first (non-stared) construction proposes to weight each score by a power of the inverse of its path length: $\omega_i = \frac{1}{p_i^{\alpha}}$, where α is a parameter. The vector is then normalized. The main criticism of this construction is the imbalance created when there are many paths of the same length (example: $\alpha = 1$, one path of length 2 totalling a weight of 1/2 and ten paths of length 3 totalling a weight of 10/3: that is to say 3/23 vs 20/23 after normalization).

To balance this, [5] also present the starred option. It fixes the total weight $T(p)$ of all paths of length p as a function of the number of paths, and to assign to each path of length p a fraction of this weight:

$$T(p) = \left(\frac{n_p}{n_p + 1}\right)^{\alpha} \cdot \left(1 - \sum_{q=1}^{p-1} T(q)\right), \quad (11)$$

where α is a parameter and n_p is the number of path of length p. Then, they define $\omega_i = \frac{T(p_i)}{n_{p_i}}$, and the vector is finally normalized.

In our case, the only difference with the original definition is to consider the paths of length 1, paths that are not considered in [5] because they are taken as references.

E. QUASI-GLOBAL OWA-BASED AGGREGATOR

After having chosen the aggregation parameters (α_t, β_t) for the calculation of the trust (resp. (α_d, β_d) for the distrust) and γ, a width search from candidate B allows retrieving n distinct non-ignorance paths leading to B, (the search can be deepened while $n < \gamma$[1]). Each path is expressed by a score (t, d, p) representing the propagation chain of the path, relative to a chosen propagator. We then define two total order on the set of propagation chains: for $s_1, s_2 \in \mathcal{BL} \times \mathbb{N}^*$, $s_1 > s_2$ iff $t_1 > t_2$ (resp. $d_1 > d_2$) for the trust part calculation (resp. distrust part). In case of equality, we choose to order them by increasing path length ($p_1 < p_2$), and finally by decreasing knowledge ($k_1 > k_2$ where k_i is the knowledge as defined below). Then we obtain the ordered vectors T (resp. D) of the trust parts (resp. distrust parts) from the scores list s.

Finally, we construct the result score of candidate B from these ordered lists as:

$$(t, d) = (\sum_i T_i \cdot \frac{wt_i \cdot \omega t_i}{\sum wt_i \cdot \omega t_i}, \sum_i D_i \cdot \frac{wd_i \cdot \omega d_i}{\sum wd_i \cdot \omega d_i}), \quad (12)$$

where wt is the OWA weight vector for the trust part, wd is the OWA weight vector for the distrust part, ωt is the path length dependent weight vector for the trust part and ωd is the path length dependent weight vector for the distrust part.

V. EVALUATION

In this section, we evaluate our new aggregator for a quasi-global reputation calculation. We start by presenting our dataset and the formatting to make it usable. We then propose two evaluation approaches. The first one consists in comparing the results with those obtained by a reference algorithm: EigenTrust. The second one is a performance evaluation based on the principle of quasi-globality: what is the minimal and sufficient amount of information to aggregate to obtain a reputation score that can be considered as global ?

A. DATA SET

The choice of dataset was motivated by two arguments. Firstly, we need a representation of a bi-valued weighted

[1]If we can't find enough paths, we can return a partial result aggregating γ_{real} paths, with the percentage $\gamma_{real}/\gamma_{target}$ as trustworthiness information.

TABLE 1. Trust degree interpretation.

Trust degree Label		τ
1	Do not know	0.00
2	Do not trust	0.00
3	Somewhat trust	0.25
4	Generally trust	0.50
5	Highly trust	0.75
6	Trust with my life	1.00

TABLE 2. Knowledge degree interpretation.

Knowledge degree Label		k
1	Not at all	0.00
2	A little bit	0.25
3	Somewhat	0.50
4	Fairly well	0.75
5	Very well	1.00
6	Extremely well	1.00
7	Could not know any better	1.00

directed graph. Indeed, the vast majority of datasets representing web-of-trust, like epinions ([20], [21], [22] and [23]), or from bitcoin network ([24], [25], [26] and [27]), are weighted by uni-valued weights. To the best of our knowledge, the dataset used in [3] and [5] is the only bi-valued dataset we could use. Secondly, the re-use of this dataset enabled us to validate the formatting of the raw data (we get the same statistics on the raw data). However, the comparison with previous results is impossible because the aggregators presented in [3] and [5] are local whereas our proposal concerns quasi-global aggregators.

The dataset is initially formatted as a list of weighted directed edges of a graph. However, the first sorting is to eliminate the irrelevant and/or null data. After this first sort, we obtain a network of 397471 users and 2697705 direct opinions. Each edge is presented as follows:

- User sending the opinion,
- User receiving the opinion,
- Trust degree, as numeric value in $[\![1, 6]\!]$,
- Knowledge degree, as numeric value in $[\![1, 7]\!]$.

The trust degree and knowledge degree are then interpreted as shown in Table. 1 and Table. 2 to define τ and k values. Finally, after defining $(\tau, k) \in [0, 1]$, we define (t, d) as:

$$(t, d) = (k \cdot \tau, k \cdot (1 - \tau)). \tag{13}$$

The Fig. 5 represents the distribution of all non-zero edges in the network. The red cross AV is the arithmetic mean at (0.42, 0.21). This value allows us to notice that direct opinions are on average twice as positive as negative. This imbalance in favor of positive opinions helps when applying Eigentrust because Eigentrust calculations only consider positive opinions. So, we know that the Eigentrust application will consider on average 2/3 of the raw data.

B. EIGENTRUST COMPARISON

In this evaluation, we choose to compare our result to the result obtained by EigenTrust. There are two major difficulties with this comparison:

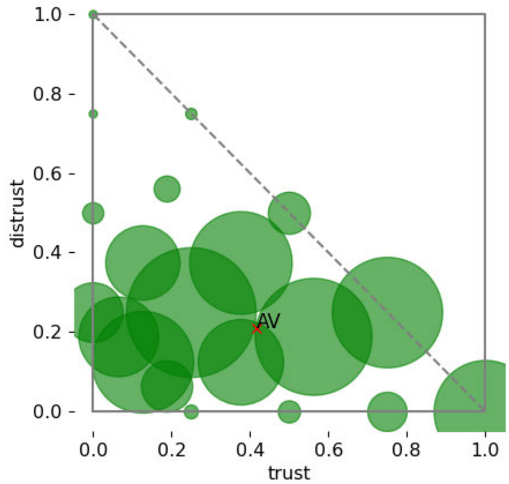


FIGURE 5. Raw data representation of the dataset. The size of the disk is proportional to the square root of the corresponding number of data. The red cross named AV is the arithmetic mean of all non-zero data.

- EigenTrust generally uses a pre-trusted peer set to improve its efficiency and permeability. In our case, we do not have this set. Therefore, we restrict our graph to its largest strong connected component in order to ensure the reliability of EigenTrust results without a pre-trusted peer set. This restriction allows us to efficiently apply Eigentrust, and thus to use the same dataset for Eigentrust and Bi-lattice model. However, this restriction is not necessary for the application of the Bi-lattice model alone.
- EigenTrust is an algorithm using uni-valued data. However, the voting information initially received by EigenTrust is: $(+1)$ for a satisfaction vote and (-1) for an unsatisfaction vote. The resulting uni-valued data is then computed as follows: $max(sat - unsat, 0)$ followed by a normalization. This degradation function then allows transforming a set of votes into a Markov process. We then choose to adopt the same degradation function to our score values: for a score $s = (t, d)$, we build the value $e = max(t - d, 0)$, then we apply the same normalization process.

We construct our comparison as follows:

- **Eigentrust:** We load the raw data by applying univalued degradation. We then restrict the graph to its largest strongly connected component (named c). We finally apply EigenTrust to obtain the global trust list of members ei.
- **Bi-lattice:** For comparison purposes, we derive the Bi-lattice graph from the EigenTrust graph. We then reload the raw bi-valued data by restricting ourselves to the strongly connected component c. For the members of the component c, we are sure that at least one notice is sent to each member because the component is also connected in the case of Bi-lattice loading. We can then search the aggregated score of each member and build the quasi-global score list of members bl (in the

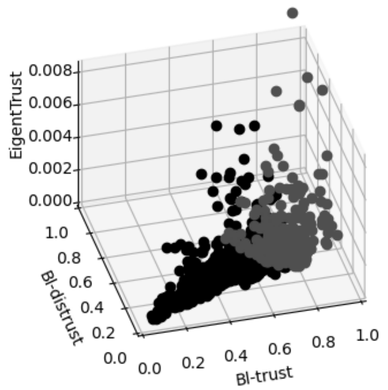


FIGURE 6. EigenTrust results (in z) in function of Bi-lattice results (in xy). Each point represents a member, and the grey points are members where the score has a knowledge greater than 1.

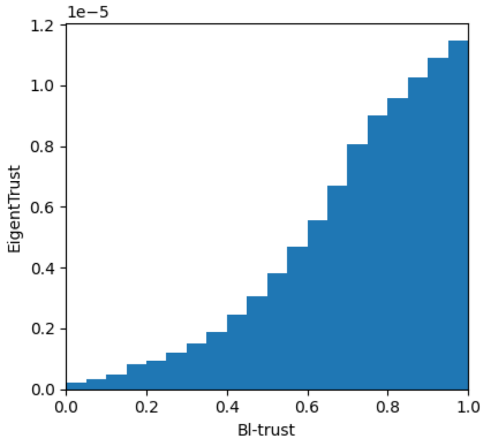


FIGURE 7. EigenTrust results (in y) in function of trust Bi-lattice results (in x). Each step is the average of the values belonging to its subdivision.

following, we consider the list of trust values bl_t and the list of degraded values bl_u)

The Fig. 6, 7, and 8, allow visualizing the results obtained with the simplest configuration : non-stared option with $\alpha_t = \alpha_d = 0$, $\beta_t = \beta_d = 0$ and $\gamma = 50$. γ is arbitrarily chosen of the order of δ^2 to ensure a search horizon $h > 1$ while keeping a reasonable computation time (a few minutes). The Fig. 6 represents only a connected component of 1000 members for readability. The two other figures (Fig. 7 and Fig. 8) are effective on the totality of the dataset, that is to say a connected component of 250276 members with 2079993 direct opinions ($\delta = 8.31$).

For example, we can interpret the results of Fig. 7 as follows: "members with a trust value for Bi-lattice in $[0.9; 0.95[$ (second last step) have on average a trust value of $1.1 \cdot 10^{-5}$ for EigenTrust".

These first comparisons show that a member with a "trustworthy" score via Bi-lattice results will on average have a high trust value via EigenTrust. And respectively, a member with an "untrustworthy" score via Bi-lattice results will on average have a low trust value via EigenTrust. At first sight, it seems that the trust value of the Bi-lattice is more representative of EigenTrust than the degraded value.

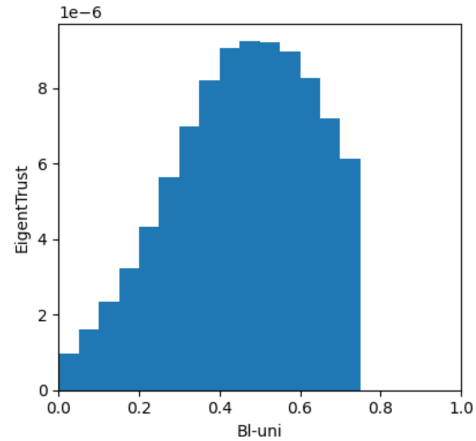


FIGURE 8. EigenTrust results (in y) in function of uni-valued degraded Bi-lattice results (in x). Each step is the average of the values belonging to its subdivision.

TABLE 3. Bi-lattice vs EigenTrust comparisons synthesis.

	All members		without last decile	
	Δ_{ei}	error %	Δ^{10}_{ei}	error %
bl_t	0.779	38.9%	0.465	25.8%
bl_u	0.750	37.5%	0.465	24.4%

To deepen the comparison, we introduce a measure of the difference between the Bi-lattice and EigenTrust results: after normalizing the Bi-lattice results (trust value or univalued), we define cumulative error as the sum of the absolute differences between two normalized numbers lists f and g:

$$\Delta_{f,g} = \sum_i abs(f_i - g_i) \in [0; 2]. \tag{14}$$

The lists used in Fig. 7 and 8 have respectively $\Delta_{bl_t,ei} = 0.779$ and $\Delta_{bl_u,ei} = 0.750$. Indeed, the histogram representation hides the number of members represented in each step. The measure Δ finally allows us to show that the univalued degradation gives results slightly closer to those of EigenTrust. In addition, we define a variant of Δ (named $\Delta^{10} \in [0, 1.8]$) that excludes the last decile from the list. Then, we obtain $\Delta^{10}_{bl_t,ei} = 0.465$ and $\Delta^{10}_{bl_u,ei} = 0.439$. This variant allows us to show that about 1/3 of the cumulative error is contributed by the 10% most erroneous. The Table. 3 summarizes these results.

In this evaluation, we do not address the issue of configuration . The results are always obtained with the simplest configuration (non-stared option with $\alpha_t = \alpha_d = 0$, $\beta_t = \beta_d = 0$ and $\gamma = 50$). Indeed, different configurations does not allow to get significantly closer to the results of EigenTrust (in general, $\Delta_{bl_t,ei}$ is around 0.8 and $\Delta_{bl_u,ei}$ is between 0.7 and 0.9). The goal of this comparison is not to find an optimal configuration , but to show that the Bi-lattice results are consistent with those obtained with EigenTrust.

C. PERFORMANCE EVALUATION AND OPTIMAL CONFIGURATION

In this evaluation, we are interested in the impacts of the γ parameter and the associated optimal configuration . The goal is to highlight the concept of quasi-globality: "What is the necessary and sufficient search depth around a candidate B to extract the majority of information about B ?"

We want to compare the results obtained for different values of γ and thus define a "good" configuration . We define $bl_{\alpha,\beta,\gamma}$ (possibly $bl_{\alpha*,\beta,\gamma}$) the scores list of members obtained with the configuration $\alpha = (\alpha_t, \alpha_d)$ (starred or non-starred option), $\beta = (\beta_t, \beta_d)$ and γ.

We can approach the definition of a "good" configuration in several different ways:

- (α, β, γ) is a "good" configuration if, for any γ' greater than γ, the results obtained for γ' are close to those of γ. This definition best represent the principle of quasi-globality. However, it has one major defect: it highlights an edge effect of the α parameter. Indeed, for large values of α (resp. small values of $\alpha*$), the associated weight vector will tend to overvalue the paths of length 1 and to neglect all the others. Thus, if all paths of length 1 are considered for $\gamma = \gamma_1$ of the order of δ, then the results for larger γ will be similar. According to this definition, all configurations with $\alpha > 10$ (resp $\alpha* < 0.1$) are "good" configurations (all the better as α is large (resp. $\alpha*$ small)).
- (α, β, γ) is a "good" configuration if, as a function of γ, the results converge quickly to a reference distribution of score. This definition seems the most reliable, but its application is complicated. Indeed, the dataset used does not have any reference distribution. Moreover, if we try to build a reference distribution with other operators (via other aggregators, uniform distribution, random distribution ...) the configuration will only try to mimic this other operator. This behavior seems desirable, but only in the case where the reference distribution is an absolute truth.
- To compensate for the lack of any reference distribution, we choose to use the dataset dating. Each dataset entry is dated from 2004 to 2009 (outliers are ignored). We choose to separate our dataset in two sub-set: from 2004 to 2005 to build a computational network named g, and from 2006 to 2009 to build a reference network named g_{ref}. Thus, we define a "good" configuration as follows: (α, β, γ) is a "good" configuration if, as a function of γ, the results computed on g converge quickly to the results computed on g_{ref} with a large γ. Thereafter, we choose to use this definition because it integrates the principle of quasi-globality (with respect to a reference distribution considered as global) and avoids the problems of the first definition.

In this evaluation, three new difficulties arise: the construction of the g and g_{ref} networks, the choice of reference distribution on g_{ref}, and the choice of measurement tools.

- To build the networks g and g_{ref}, we have to respect several constraints:
  - The two networks must be strongly connected.[2] To do this, we start to build two large graphs and restrict the larger one to the connected component of the smaller one, and so on until the graphs have the same members. The chosen graphs for this evaluation are restricted to 1000 members by computational constraints.
  - The two networks must not have common edges: this constraint is ensured by the choice of the dates. Graph g has only opinion before 2006 and g_{ref} has only opinions after 2007.
  - The two graphs must have similar topology: we want $\delta_g \approx \delta_{g_{ref}}$ and the average of the shortest path between all members to be similar. We define $\bar{l}$ the average of all the shortest paths (excluding the paths of length 0) and l_{max} the longest of the shortest paths.
- To establish the reference distribution on g_{ref}, we rely on two assumptions:
  - The opinions issued between 2006 and 2009 are dependent on the existing opinions from 2004 to 2005.
  - A quasi-global aggregation calculation with a large γ is close to a global aggregation calculation (i.e. a large γ allows integrating the opinions of all the members of the network).

  Thus, we define $\gamma_{max} = \lceil \delta^{\bar{l}} \rceil$. This value of γ allows on average to aggregate at least one notice from all members of the network. So, the aggregation parameterized by (α, β, γ) calculated on g will then be compared to the aggregation parameterized by $(\alpha, \beta, \gamma_{max})$ on g_{ref}.
- To compare the results on g to the reference on g_{ref}, we choose to use one of the measures proposed by [3] and [5]: mean absolute error ($MeanAE$) in [0; 2], define by (15). In addition, we choose to introduce two other measures to better understand the distribution of errors: max absolute error ($MaxAE$) in [0; 2], define by (16), and the average excluding the ten most erroneous percent ($MeanAE^{10}$) in [0; 1, 8].

$$MeanAE = \frac{\sum_{i=1}^{p} |t_i - t'_i| + |d_i - d'_i|}{p} \tag{15}$$

$$MaxAE = max_{i=1}^{p}(|t_i - t'_i| + |d_i - d'_i|) \tag{16}$$

The first observation focuses on the variations between the starred and non-starred options, Fig. 9 shows some examples. The starred options were quickly eliminated from the comparison process because they present on average (i.e. relative to MeanAE) less convergent results than the

[2] The connection of our graph is appreciated but not necessary, indeed, it is enough that the members are receivers to compute their score. However, the connection guarantees that there are many different paths to each member and thus that all computations remain successful (i.e. $\gamma_{reel} = \gamma_{target}$) even for large values of γ.

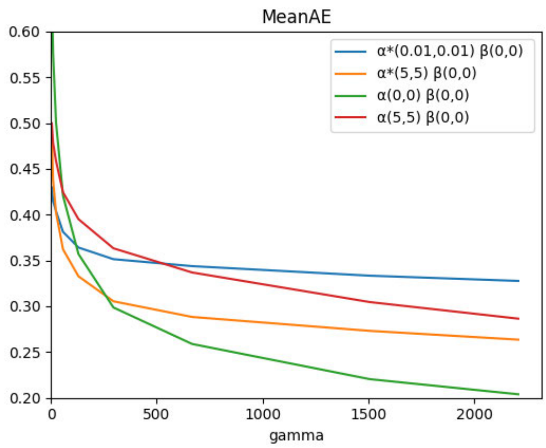


FIGURE 9. Example of measures with *MeanAE* of some configurations with two starred options and two non-starred options.

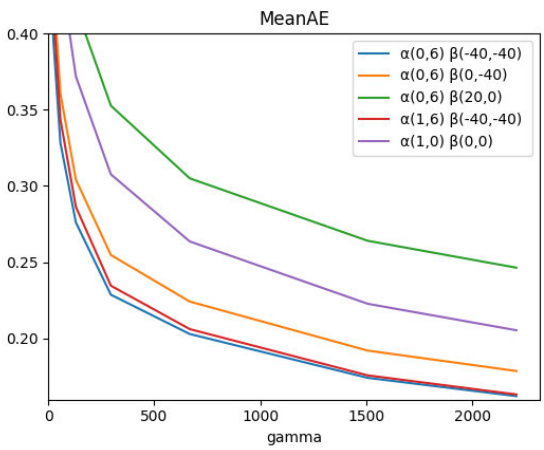


FIGURE 10. Results obtained with *MeanAE* measure.

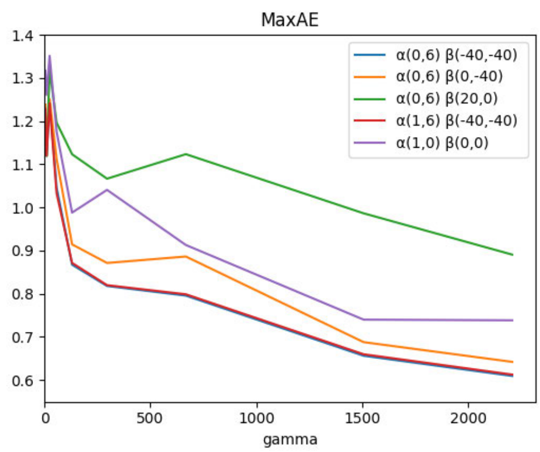


FIGURE 11. Results obtained with *MaxAE* measure.

non-starred options.[3] Although their results can be better for small γ, the results are chaotic and the relevance of the α parameter is very limited when γ is very small. For these different reasons, the following evaluation only concerns the non-starred options.

[3]In fact, the starred option converges quickly, but to a more distant value than the non-starred option.

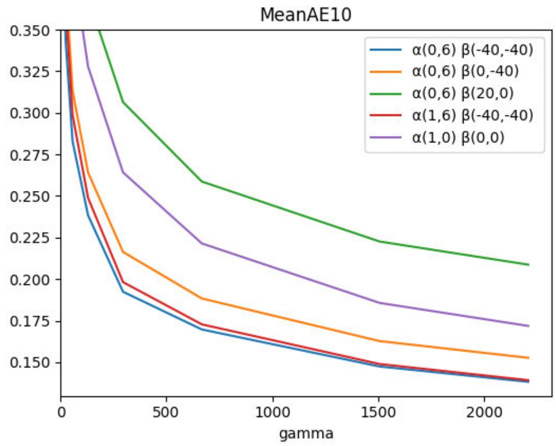


FIGURE 12. Results obtained with *MeanAE*^{10} measure.

TABLE 4. Synthesis of measures for the best configuration (lower blue curve on Fig. 10, 11, and 12).

	$MeanAE$		$MeanAE^{10}$		$MaxAE$	
γ	value	%	value	%	value	%
11	0.462	23.1%	0.417	23.1%	1.122	56.1%
58	0.328	16.4%	0.283	15.7%	1.046	52.3%
296	0.229	11.4%	0.192	10.7%	0.818	40.9%
1507	0.174	8.7%	0.148	8.2%	0.656	32.8%
2208	0.162	8.1%	0.138	7.7%	0.609	30.5%

To draw the resulting curves, many configurations have been tested: $\alpha \in [0, 15]$ with smalls steps close to zero ($\alpha = 15$ is considered as limit case representing all the $\alpha > 15$ cases); $\beta \in [-40, 40]$ with a step of 5 ($\beta = -40$ or $\beta = 40$ are considered as limit cases in terms of computational capacity). We have tested several thousand of configurations , and the Fig. 10, 11, and 12 show some different results for the three measurements. The blue curve with configuration $\alpha = (0, 6)$ and $\beta = (-40, -40)$ achieves the best performance in almost all measures.[4] The Table. 4 below summarizes this curve values for several γ.

Because of the construction of the measures, the impacts of α_t and β_t are independent of α_d and β_d. The results can thus be analyzed independently for the trust and for the distrust:

- **Trust analysis:** $\alpha_t = 0$ and $\beta_t = -40$
  These results are both limit cases. They can be interpreted as follows: $\alpha = 0$ implies that there is no weighting of the trust values according to the length of the path with the candidate. A small value of α confirms an already well known idea: trust is transitive (e.g., even if A is far from B in the network, if A attributes trust to B, then this trust is perceptible in the aggregation of B's score). $\beta = -40$ represents a case where the sub OWA operator assigns the same weight to all aggregated trust values. Synthetically, the most relevant aggregator for the trust part is very similar to AV, it is an unweighted arithmetic average. However, there is a small difference with AV because, in our aggregation, the search for γ

[4]$\alpha_d = 6$ is a rounded value. The tests revealed that $\alpha_d = 5.9$ proposed a very slight improvement of the results when γ is small, against $\alpha_d = 6.2$ when γ increases.

non-ignoring paths ensures that there will be no (0,0) in average calculation, and thus the aggregation really represents γ distinct opinion.

- **Distrust analysis:** $\alpha_t = 6$ and $\beta_t = -40$
$\alpha = 6$ implies that there is a strong weighting of the distrust according to the length of the path with candidate B. This is a strong value of α which favors very much the paths of length 1 (the paths of length 2 have a small impact and higher lengths are almost neglected). This value gives distrust a different status than trust: distrust would not be transitive or not very transitive. Direct distrust opinions have a strong impact on the calculation of the score whereas indirect opinions are strongly diminished. The analysis of β is the same as for trust.

VI. CONCLUSION

The use of multivalued reputation models is still underdeveloped in the literature. Moreover, the notion of quasi-global reputation is, to our knowledge, never used yet. The concept of globality itself still lacks some formalism because of its double meaning.

In this paper, based on commonly accepted definitions for the notions of local trust and global trust, we propose a formalization of the concept of quasi-global trust. In the first evaluation, we chose to compare this concept to a global reputation reference model. We have developed a protocol to compare the bivalued Bi-lattice model to the univalued Eigentrust model. We have chosen to consider several interpretations of the couple (t, d) and have shown that the comparison of the distributions ei (obtained with Eigentrust model) and bl_u (obtained by $t - d$ subtraction with Bi-lattice model) produces consistent results: a member with a high value in ei has, on average, a high value in bl_u.

In a second evaluation, we choose to focalize on the Bi-lattice model for several purposes. On the one hand, we extend the notion of the quantity of information (knowledge of score), and thus of reliability, to the idea of quasi-globality and to its associated error. We show that it is possible to approach results considered as global by strongly minimizing the calculations, while keeping a good reliability. On the other hand, the interpretation of the results of several configuration allowed us to highlight an important difference between trust and distrust: trust would be transitive whereas distrust would not.

In summary, we propose a new operator for the Bi-lattice based model to evaluate reputations in human network contexts. Moreover, the high configurbility of our operator allows for lightweight computational options that highlight the advantages of quasi-globality.

This article then proposes a first approach to the concept of quasi-globality, but it can be improved. One of the most important aspects is the relevance of the used dataset. The dataset has a large amount of middle data (see on Fig. 5), as much in the conviction of opinions (value of k), as in the proportion of trust/distrust. Moreover, the reference distribution is built from a subset of the dataset. Thus, the results are highly dependent on this dataset. In addition, the first tests were performed on graphs of 200 members and the final evaluation was confirmed on graphs of 1000 members (the main motivation is to save computing time). However, the dataset contains information about 397471 users, and the largest common components found for g and g_{ref} is 53436 users.

A. FUTURE WORKS

This work also suggests a number of avenues for future work, particularly with regard to the choice of path calculation and potential applications to distributed networks.

In the path search, we chose not to consider paths with loops as in [19]. The main goal is to avoid the obvious malicious coalition attack. However, it could be interesting to deepen the results by measuring the impact of these loops, notably by distinguishing loops containing the candidate from those that do not.

Before the score aggregation, we choose to use the PR_3 propagator to propagate our scores along the path. This propagator tends to make the knowledge drop quickly ($k(PR_3(x, y)) = k(x) \cdot k(y) - 2 \cdot t_x \cdot d_x \cdot t_y \cdot d_y$). This decrease is moreover accentuated by the fact that our dataset contains only few convinced opinions (i.e. $t = 0$ or $d = 0$). Other propagators, more stable concerning the evolution of knowledge, could give different results and will be investigated in future work.

A new dimension of the work could focus on the development of multivaluation and its adapted propagators. Particularly adapted when using the model for various cases, it would be interesting to differentiate several values of trust and/or distrust (for example, a score like $(t_1, t_2, t_3, \ldots, d_1, d_2, d_3, \ldots)$ where (t_i, d_i) is a bi-value relative to a given theme).

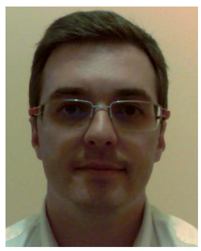
Finally, we do not address the issue of decentralization in this paper. Indeed, some networks, like BitTorrent file exchange or blockchain-based networks, do not depend on a centralized unit. The usability of a trust model is then directly linked to their distributivity. EigenTrust is one of the reference of efficiently distributable reputation model. Its principle is to allocate the responsibility of a computation to members who have no interest in it (with redundancy), and that each member transmits these results to the next to perform the computation. The responsibility of "who calculates what" is then stored in a distributed hash table (DHT) accessible by everyone. In our case, we suggest that each member takes the responsibility of storing some score value of the network (only the direct opinions, the chains of propagation are always recalculated). The main problem to solve is to know "who have given an opinion to whom ?" To do this, we assign storage responsibilities: each member stores all the opinions converging to a small sub-list of members (this sub-list being deduced from a public DHT). Thus, when a requester is interested in the opinions converging to a candidate B, the DHT tells him who is responsible for storing these score values. The propagation and aggregation calculations are then his responsibility. We think that the use of a quasi-global aggregator is well suited to a decentralized network, as the γ parameter (chosen by the requester) limits the amount of raw information required to perform the aggregation. In this way, our aggregator offers good synergy with the concept of decentralization, by limiting the number of exchanges required between members.

REFERENCES

[1] S. Ruohomaa and L. Kutvonen, "Trust management survey," in *Trust Management*, P. Herrmann, V. Issarny, and S. Shiu, Eds. Berlin, Germany: Springer, 2005, pp. 77–92.
[2] M. De Cock and P. P. da Silva, "A many valued representation and propagation of trust and distrust," in *Fuzzy Logic and Applications*, I. Bloch, A. Petrosino, and A. G. B. Tettamanzi, Eds. Berlin, Germany: Springer, 2006, pp. 114–120.
[3] P. Victor, C. Cornelis, M. De Cock, and E. Herrera-Viedma, "Practical aggregation operators for gradual trust and distrust," *Fuzzy Sets Syst.*, vol. 184, no. 1, pp. 126–147, Dec. 2011. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0165011410004355
[4] P. Victor, C. Cornelis, M. De Cock, and P. Pinheiro da Silva, "Gradual trust and distrust in recommender systems," *Fuzzy Sets Syst.*, vol. 160, no. 10, pp. 1367–1382, May 2009. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0165011408005290
[5] N. Verbiest, C. Cornelis, P. Victor, and E. Herrera-Viedma, "Trust and distrust aggregation enhanced with path length incorporation," *Fuzzy Sets Syst.*, vol. 202, pp. 61–74, Sep. 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0165011412000905
[6] C. A. Haydar, "Les systèmes de recommandation à base de confiance," M.S. thesis, LORIA, Université de Lorraine, Nancy, France, Sep. 2014. [Online]. Available: https://hal.univ-lorraine.fr/tel-01751172
[7] S. Castaldo, *Trust in Market Relationships*. U.K.: Edward Elgar, 2007.
[8] F. A. Azzedin, "Trust modeling and its applications for peer-to-peer based systems," Ph.D. dissertation, Univ. Manitoba, Winnipeg, MB, Canada, 2004.
[9] F. Azzedin and M. Ghaleb, "Internet-of-Things and information fusion: Trust perspective survey," *Sensors*, vol. 19, no. 8, p. 1929, Apr. 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/8/1929
[10] F. Azzedin, "Taxonomy of reputation assessment in peer-to-peer systems and analysis of their data retrieval," *Knowl. Eng. Rev.*, vol. 29, no. 4, pp. 463–483, Sep. 2014.
[11] J. Guo, I.-R. Chen, and J. J. P. Tsai, "A survey of trust computation models for service management in Internet of Things systems," *Comput. Commun.*, vol. 97, pp. 1–14, Jan. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366416304959
[12] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proc. 12th Int. Conf. World Wide Web*. New York, NY, USA: Association for Computing Machinery, 2003, pp. 640–651.
[13] J. Li, X. Wang, B. Liu, Q. Wang, and G. Zhang, "A reputation management scheme based on global trust model for peer-to-peer virtual communities," in *Advances in Web-Age Information Management*, J. X. Yu, M. Kitsuregawa, and H. V. Leong, Eds. Berlin, Germany: Springer, 2006, pp. 205–216.
[14] X. Fan, L. Liu, M. Li, and Z. Su, "EigenTrustp^{++}: Attack resilient trust management," in *Proc. 8th Int. Conf. Collaborative Comput., Netw., Appl. Worksharing*, Dec. 2012, pp. 416–425.
[15] L. Xiong and L. Liu, "A reputation-based trust model for peer-to-peer e-commerce communities," in *Proc. IEEE Int. Conf. E-Commerce*, Mar. 2003, pp. 275–284.
[16] L. Xiong and L. Liu, "PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Trans. Knowl. Data Eng.*, vol. 16, no. 7, pp. 843–857, Jul. 2004.
[17] R. Chen, X. Zhao, L. Tang, J. Hu, and Z. Chen, "Cuboidtrust: A global reputation-based trust model in peer-to-peer networks," in *Autonomic and Trusted Computing*, B. Xiao, L. T. Yang, J. Ma, C. Müller-Schloer, and Y. Hua, Eds. Berlin, Germany: Springer, 2007, pp. 203–215.
[18] H. A. Kurdi, "HonestPeer: An enhanced EigenTrust algorithm for reputation management in P2P systems," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 27, no. 3, pp. 315–322, Jul. 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1319157815000440
[19] P. Avesani, P. Massa, and R. Tiella, "A trust-enhanced recommender system application: Moleskiing," in *Proc. ACM Symp. Appl. Comput.* New York, NY, USA: Association for Computing Machinery, Mar. 2005, pp. 1589–1593, doi: 10.1145/1066677.1067036.
[20] *Dataset Soc-Epinions1.Txt.Gz*. Accessed: Oct. 2022. [Online]. Available: https://snap.stanford.edu/data/soc-Epinions1.html
[21] M. Richardson, R. Agrawal, and P. M. Domingos, "Trust management for the semantic web," in *Proc. Int. Workshop Semantic Web*, 2003, pp. 351–368.
[22] *Dataset Soc-Sign-Epinions.Txt.Gz*. Accessed: Oct. 2022. [Online]. Available: https://snap.stanford.edu/data/soc-sign-epinions.html
[23] J. Leskovec, D. Huttenlocher, and J. Kleinberg, "Signed networks in social media," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.* New York, NY, USA: Association for Computing Machinery, 2010, pp. 1361–1370, doi: 10.1145/1753326.1753532.
[24] *Dataset Soc-Sign-Bitcoinotc.Csv.Gz*. Accessed: Oct. 2022. [Online]. Available: https://snap.stanford.edu/data/soc-sign-bitcoin-otc.html
[25] S. Kumar, F. Spezzano, V. S. Subrahmanian, and C. Faloutsos, "Edge weight prediction in weighted signed networks," in *Proc. IEEE 16th Int. Conf. Data Mining (ICDM)*, Dec. 2016, pp. 221–230.
[26] *Dataset Soc-Sign-Bitcoinalpha.Csv.Gz*. [Online]. Available: https://snap.stanford.edu/data/soc-sign-bitcoin-alpha.html
[27] S. Kumar, B. Hooi, D. Makhija, M. Kumar, C. Faloutsos, and V. S. Subrahmanian, "REV2: Fraudulent user prediction in rating platforms," in *Proc. 11th ACM Int. Conf. Web Search Data Mining*, 2018, pp. 333–341.

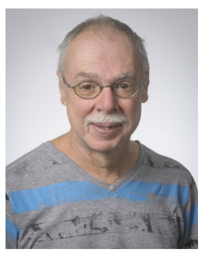
BAPTISTE BELTZER received the B.S. degree in sociology, the B.S. degree in mathematics, and the M.S. degree in cryptography from the University of Limoges, France, in 2020. He is currently pursuing the Ph.D. degree in computer science with the Domus Laboratory, University of Sherbrooke, Sherbrooke, QC, Canada.

His research interests include the study of digital social networks and the protection of personal data on such networks; especially in the context of decentralized computing, such as blockchain technologies, consensus algorithms, and reputation models.



EMMANUEL CONCHON received the M.Sc. and Ph.D. degrees in wireless communication from the "Institut National Polytechnique de Toulouse" (INPT), Toulouse, France, in 2002 and 2006, respectively.

In September 2008, he joined Champollion University as an Associate Professor and the Institut de Recherche en Informatique de Toulouse (IRIT) as a Researcher. Since September 2015, he has been an Associate Professor with the University of Limoges and a Researcher with XLIM. His research interests include security solutions for wireless networks, context-aware systems, and secure middleware solutions for health applications.



SYLVAIN GIROUX received the Ph.D. degree in computer science from the University of Montreal, in 1993. He is currently a Professor with the Department of Computer Science, University of Sherbrooke, Canada. His professional experience is well-balanced between academic institutions and private corporations. His current research interests include cognitive assistance, smart homes, the Internet of Things, ontologies, activity recognition, augmented reality, cryptocurrencies, aging at home, and transdisciplinary research.