

# A Framework for Trust and Distrust Networks

Krishnaprasad Thirunarayan  
Department of Computer Science and Engineering  
Wright State University, Dayton, OH 45435  
t.k.prasad@wright.edu  
<http://www.cs.wright.edu/~tkprasad>  
937-775-5109

Rakesh Verma  
Computer Science Department  
University of Houston, Houston, TX 77204-3010  
rverma@uh.edu  
<http://www.cs.uh.edu/~rmverma>  
713-743-3348

## Abstract

In this age of internet and electronic commerce it is becoming increasingly important to have and to manipulate information about the trustworthiness of the content or service providers in order to make informed decisions. This paper explores realistic models of trust and distrust based on partially ordered discrete values and proposes a framework, which is sensitive to local, relative ordering of values rather than their magnitudes. The framework distinguishes between direct and inferred trust, preferring direct information over possibly conflicting inferred information. It also represents ambiguity or inconsistency explicitly. The framework is capable of handling general trust and belief networks containing cycles.

## 1 Introduction

Searching for information on the World Wide Web usually retrieves a large number of documents. The precision and reliability of the returned results can be improved by ranking and summarizing the documents, taking into account (i) the relevance of the content to the query (traditional IR), (ii) the collective Web support implicit in the link-structure of the documents (pagerank), (iii) the user trust in the document source, and (iv) the nature of endorsement (positive or negative) (link semantics).

Given a documents database and a query, information retrieval systems return a subset of documents ordered by decreasing relevancy. Furthermore, it is becoming increasingly important to have information about the trustworthiness of the content providers before we can make informed decision about the content (or product or seller) obtained as search results. This is becoming increasingly critical in the face of (unethical) search engine optimization techniques such as keyword stuffing, hidden/duplicate text, spamdexing, etc employed to boost “content” relevance. In Section 2, we provide some background on the structure of trust values. In Section 3, we investigate approaches to representing and determining source (and thereby content) trustworthiness information that we expect will play an important role in building next generation information retrieval systems and Web 3.0.

## 2 Background: The Structure of Trust

Traditional approaches to formalizing trust between a pair of users models trust as a real number in the closed interval  $[0,1]$ . Even though this facilitates trust computation, such as via aggregation and propagation, there are inherent difficulties in coming up with initial trust values and semantically justifying computed trust values. Furthermore, these are too fine-grained and force a total order on trust values. To paraphrase Guha et al [9]: *While continuous-valued trusts are mathematically clean [15], from the standpoint of usability, most real-world systems will in fact use discrete values at which one user can rate another.* Furthermore, it is not unreasonable to expect and allow users to specify relative trust and distrust information. We propose to explore “realistic” models of trust and distrust based on partially ordered discrete values. Our approach differs from existing works ([9, 13, 15] to name a few recent ones) as follows:

- We model both trust and distrust among users explicitly as *discrete* values.
- Our approach is sensitive to *local, relative* ordering of trust values rather than their magnitudes.
- We distinguish between *direct* trust and *inferred* trust, letting direct information override conflicting inferred information.
- We regard *equal* or *incomparable* evidence in support and against a user as ambiguous/inconsistent/ambivalent trust, and represent it explicitly. (Ambiguous trust implies that further investigation is necessary to determine whether or not to trust the user.)

We believe that this approach provides a natural representation of *relative* trust information a user (aggregator) has, which can also be used for initialization. For instance, trust based on direct knowledge is superior to trust based on a stamp of approval from a certifying agency. However, it may not always be possible to determine relative trustworthiness of two arbitrary sources<sup>1</sup>. As an example, consider the conflicting descriptions of the same events given by Clarence Thomas and Anita Hill in the (in)famous 1991 confirmation hearings of the Supreme Court Justice Clarence Thomas which cannot be resolved beyond reproach either way. In this situation, our proposal enables representation of ambivalence as opposed to requiring one to break the tie. Note also that in practice, trust relationships can change over time as new information arrives, causing *non-monotonic* changes to inferred trust information.

Epinions dataset has been used by several prior works for experimental evaluation [6]. `epinions.com` is a website where people can review products. Users can add other users to their "Web of Trust", i.e., reviewers whose reviews and ratings they have consistently found to be valuable and their "Block list", i.e., authors whose reviews they find consistently offensive, inaccurate, or in general not valuable. Trust and distrust are materialized as 1 and -1. Richardson et al [15] start with Epinions user trust graph, *synthetically* generate real-valued trust values using user quality parameter, and belief information using user reviews data, to study the relationship between user quality and trust propagation. Massa and Hayes [13] make a case for distinguishing (referential) hyperlinks into two categories: positive endorsement links and negative criticizing links. PageRank algorithm [4] is run on Epinions user trust graph with various combination of trust and distrust links, to analyze the effect of added expressiveness on user rankings. Guha et al [9] encode trust and distrust information as 1 and -1, and define four different atomic operations for propagating trust: direct propagation, co-citation, transpose trust and trust-coupling. These operations are captured via matrix operations. Their framework works for real-valued trust caused by additional parameters involved in combining the atomic propagations. Final trust/distrust values are determined using finite number of iterations (finite length paths) and thresholds for rounding that uses initial proportions of trust and distrust. Zeigler and Lausen [23] presents a classification of trust metrics to evaluate "transitivity of trust through social networks". Wang and Singh [20, 21] propose a probability of probabilities approach to trust that represents uncertainty information explicitly and belief/trust as real numbers between 0 and 1. Their approach as well as other real-valued approaches to aggregation and propagation could be used in our framework to determine the partial ordering information.

---

<sup>1</sup>We can always generate a total order from a partial order but that brings in some arbitrariness.

Artz and Gil [1] surveys models of trust, different definitions of trust, trust metrics, and their specific determination using policies or reputation.

Massa and Avesani [14] analyze the variation in average trust values for different equivalence classes of users, determined on the basis of path length. Golbeck and Hendler [8] describe a more sophisticated approach to locally inferring trust in web-based social networks that explicitly represents both trust and no trust on a fixed linear scale obtained from context-based ratings, and aggregates trusts from neighbors via weighted averaging. Similarly, the approach of Bintzios et al [3] also infers a trust value for an information source from a combination of only the direct trust values of its neighbours using path algebra operators such as maximum and multiplication. In [10], Katz and Golbeck want to compute a partially ordered priority relationship among competing defaults using the trust computations described in Golbeck and Hendler [8]. They do not show how to leverage the partial order itself to get a new framework for computing trust values as we do in this paper.

In contrast with these approaches, our work develops a computational model of trust and distrust among users (resp. belief and disbelief among statements) that abstracts weights on links through local partial ordering of links, and propagates (dis)trust (resp. (dis)belief) information via local distributed computation. Our approach emphasizes local scope and local computation, to determine global trust (resp. belief) values. It is robust with respect to redundant links obtained by replacing a node with a pair of synonymously named connected nodes. The discretization of (dis)trust (resp. (dis)belief) values, context-based partial ordering, and trust aggregation via least-upper bound operation, enables us to readily see the semantic consequences of the trust-belief network and the computational properties such as locality, convergence, etc. To summarize, our work emphasizes local relative ordering of trust/belief information to arrive at a conclusion in preference to global or absolute weights. Furthermore, on concrete examples, there are points of agreement and points of subtle disagreement.

### **3 Trust-Belief Networks and Their Semantics**

We now investigate representation and reasoning with trust and belief. For simplicity, trust is regarded as a binary relation on users and belief is regarded as a binary relation from user to statement. A user may or may not trust one another because of their firsthand experiences, or on the basis of experiences of other users they trust. In order to formalize these aspects, we introduce trust-belief networks as a graph involving user nodes connected among themselves by trust and distrust links, and to statement nodes by belief and disbelief links.

The semantics of links can be captured by formalizing trust relation among

user nodes and belief relation between user nodes and statement nodes using various paths in the network. For instance, if user  $u_1$  trusts user  $u_2$ , and user  $u_2$  trusts user  $u_3$ , it may be reasonable to tentatively assume that user  $u_1$  trusts user  $u_3$ . However, if we already know that user  $u_1$  distrusts user  $u_3$ , then the latter fact should dominate the former conclusion. It is also possible that user  $u_1$  gets conflicting information from two trusted users  $u_2$  and  $u_3$  about user  $u_4$ , and so, user  $u_1$  chooses to remain ambivalent about user  $u_4$ . (A similar argument can be put forth for determining belief in statements.)

We interpret direct links (paths of length 1) as *strict* while paths of lengths 2 or more as *defeasible*, overridden by stronger conflicting links. One can capture differing semantics of trust and belief formation based on differing intuitions they embody. For instance:

**Neighbor-oriented trust:** User  $u$  can trust user  $v$  by virtue of trust that user  $u$ 's "direct" trusted neighbors have in user  $v$ . Furthermore, the trust formation may take into account the existence or the count of trust and distrust links. This is analogous to someone seeking recommendations from their neighbors or friends about an electrician or a plumber that the latter have heard about but not necessarily experienced. We refer to these two semantics as *Top-Down-Existence* and *Top-Down-Count*.

**Topic-oriented belief:** User  $u$  can believe in statement  $s$  by virtue of "direct" beliefs bestowed on the statement  $s$  by users that user  $u$  trusts. Furthermore, the belief formation may take into account the existence or the count of trusted users that believe in statement  $s$ . This is analogous to a potential T.V. buyer seeking recommendations from those who have already purchased a particular brand of T.V. (or via reviews from corresponding `amazon.com` pages.) We refer to these two semantics as *Bottom-Up-Existence* and *Bottom-Up-Count*.

There are many interesting topological and conceptual similarities between boolean trust-belief networks and mixed inheritance networks (that we have explored in depth in the past) [11, 12, 16, 17, 19, 22]. Both kinds of graphs have links that can be positive or negative, with potential for conflicts, bringing up issues of ambiguity/inconsistency, and conflict resolution strategies. Semantics of inheritance networks can be local or ground local, be visualized using bottom-up individual flow or top-down property flow [18], analogous to the bottom-up topic-oriented belief vs top-down neighbor-oriented trust. Thus, we can explore adapting existing *local* (that is, the semantics of a node is completely determined by the semantics of its neighboring nodes and the connecting links [17]) and path-based strategies for inheritance reasoning, to deal with trust and belief.

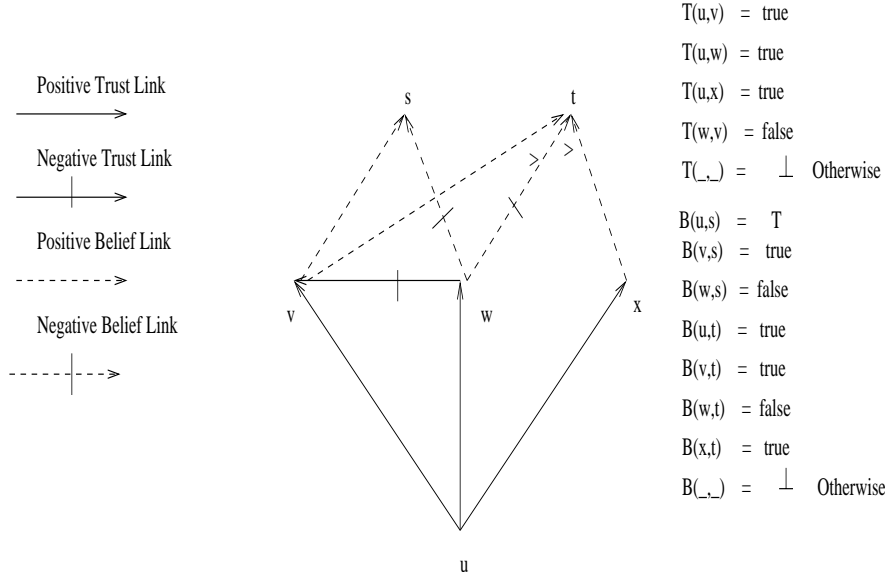


Figure 1: DAG structured Trust-Belief Network

We formalize various intuitions behind trust and belief aggregation in terms of paths in the trust network as follows.

**Definition 1** A trust-belief network is an ordered graph  $G = (UN, SN, PTL, NTL, PBL, NBL)$  containing user nodes  $UN$ , statement nodes  $SN$ , positive trust links  $PTL$  ( $\subset UN \times UN$ ), negative trust links  $NTL$  ( $\subset UN \times UN$ ), positive belief links  $PBL$  ( $\subset UN \times BN$ ), and negative belief links  $NBL$  ( $\subset UN \times BN$ ). Furthermore, for each user node  $u$  in  $UN$ , a local trust ordering relation  $\prec_u$  on its out-links to other user nodes (that is,  $\{ (u, v) \mid (u, v) \in PTL \cup NTL \}$ ), and for each statement node  $s$  in  $SN$ , a local belief ordering relation  $\triangleleft_s$  on its in-links (that is,  $\{ (u, s) \mid (u, s) \in PBL \cup NBL \}$ ). For completeness,  $PTL \cap NTL = \emptyset$ ,  $PBL \cap NBL = \emptyset$ , and  $\prec_u$  and  $\triangleleft_s$  are irreflexive/strict partial order.

We may abbreviate user node as *user*, statement node as *statement*, positive trust link as *trust link*, negative trust link as *distrust link*, positive belief link as *belief link*, and negative belief link as *disbelief link*, when there is no ambiguity. Given a link  $(u, v)$ , we say that  $u$  is a *predecessor* of  $v$  and  $v$  is a *successor* of  $u$ .

In order to develop formal semantics and efficient (one-pass, linear) computation procedure, we initially restrict the subgraph spanned by trust and distrust links to be directed-acyclic graph (DAG). See Figure 1. Subsequently, we relax this restriction, allowing cycles in trust/distrust graph. Unfortunately, as explained later,

this expressiveness brings with it quadratic complexity, in the worst case.

We model trust function  $\mathcal{T}$  and belief function  $\mathcal{B}$  supported by the trust-belief network as:

$$\begin{aligned} \mathcal{T} &: UN \times UN \rightarrow \{\perp, true, false, \top\} \text{ and} \\ \mathcal{B} &: UN \times SN \rightarrow \{\perp, true, false, \top\}. \end{aligned}$$

The values  $\perp, true, false$  and  $\top$  correspond to no information, supporting information, opposing information, and inconsistent/ambiguous information respectively. These four values can be partially ordered on information-content scale, similarly to Belnap's 4-valued logic [2]:  $\perp < true, \perp < false, true < \top$ , and  $false < \top$ . (Also, let  $[V1 < V2 \text{ iff } V2 > V1]$ , and  $[V1 \geq V2 \text{ iff } (V1 > V2) \text{ or } (V1 = V2)]$ ).

We provide count-based semantics of trust and belief aggregation by defining when user  $u_i$  can (dis)trust user  $u_j$  and when user  $u_i$  can (dis)believe statement  $s_j$ . (Note that the local trust ordering relation  $\prec_u$  on out-links of user  $u$  and  $\triangleleft_s$  on in-links of statement  $s$  appear prominently in both semantics.) We can then define trust and belief functions  $\mathcal{T}$  and  $\mathcal{B}$  in each case as follows. (Actual detailed definitions of “can (dis)trust” and “can (dis)believe” for the different cases are given later.)

**Reflexivity:** Users trust themselves.  $\forall u \in UN: \mathcal{T}(u, u) = true$ .

**(Dis)Trust-related:**  $\forall u_i, u_j \in UN$ :

- Trust:**  $\mathcal{T}(u_i, u_j) = true$  if  
 $(u_i \text{ can trust } u_j) \wedge \text{not } (u_i \text{ can distrust } u_j)$
- Distrust:**  $\mathcal{T}(u_i, u_j) = false$  if  
 $(u_i \text{ can distrust } u_j) \wedge \text{not } (u_i \text{ can trust } u_j)$
- Ambivalence:**  $\mathcal{T}(u_i, u_j) = \top$  if  
 $(u_i \text{ can trust } u_j) \wedge (u_i \text{ can distrust } u_j)$
- Ignorance:**  $\mathcal{T}(u_i, u_j) = \perp$ , otherwise.

**(Dis)Belief-related:**  $\forall u \in UN, \forall s \in SN$ :

- Belief:**  $\mathcal{B}(u, s) = true$  if  
 $(u \text{ can believe } s) \wedge \text{not } (u \text{ can disbelieve } s)$
- Disbelief:**  $\mathcal{B}(u, s) = false$  if  
 $(u \text{ can disbelieve } s) \wedge \text{not } (u \text{ can believe } s)$
- Ambivalence:**  $\mathcal{B}(u, s) = \top$  if  
 $(u \text{ can believe } s) \wedge (u \text{ can disbelieve } s)$

**Ignorance:**  $\mathcal{B}(u, s) = \perp$ , otherwise.

The rationale is that if the trust/belief is “well-defined” then there is no harm in subscribing to it but when there is some doubt due to conflicting evidence, it is better to note the ambiguity for further investigation. Note that if there is direct positive (resp. negative) trust link from  $u_i$  to  $u_j$  then  $\mathcal{T}(u_i, u_j) = true$  (resp.  $\mathcal{T}(u_i, u_j) = false$ ). Similarly, if there is direct positive (resp. negative) belief link from  $u$  to  $s$  then  $\mathcal{B}(u, s) = true$  (resp.  $\mathcal{B}(u, s) = false$ ).

### 3.1 Count-based Semantics for DAGs

We specify how trust and distrust can be propagated top-down, and how belief can be computed bottom-up through the DAG-structured trust-belief networks. This approach takes into account both the polarity and the cardinality of the “appropriate” links.

**Evidence in support of Trust:**  $u_i$  can trust  $u_j$  if there is an explicit trust link from  $u_i$  to  $u_j$ , or there are more of most-trusted successors  $u_k$  of  $u_i$  that trust  $u_j$  rather than distrust  $u_j$ . In other words, for the purposes of  $u_j$ , there are more endorsements than disapprovals via  $u_i$ ’s successors. ( $\| \dots \|$  stands for set-cardinality operator.)

$\forall u_i, u_j \in \text{UN}: u_i$  **can trust**  $u_j$  if

$$(u_i, u_j) \in \text{PTL} \quad \vee$$

[

$$\begin{aligned} & \| \{ (u_i, u_k) \in \text{PTL} \mid \mathcal{T}(u_k, u_j) = true \\ & \quad \wedge \neg \exists u_l \in \text{UN} : (u_k \prec_{u_i} u_l) \wedge (u_i, u_l) \in \text{PTL} \\ & \quad \wedge \mathcal{T}(u_l, u_j) = false \} \| \end{aligned}$$

is greater than

$$\begin{aligned} & \| \{ (u_i, u_k) \in \text{PTL} \mid \mathcal{T}(u_k, u_j) = false \\ & \quad \wedge \neg \exists u_l \in \text{UN} : (u_k \prec_{u_i} u_l) \wedge (u_i, u_l) \in \text{PTL} \\ & \quad \wedge \mathcal{T}(u_l, u_j) = true \} \| \end{aligned}$$

]

**Evidence in support of Distrust:**  $u_i$  can distrust  $u_j$  if there is an explicit distrust link from  $u_i$  to  $u_j$ , or there are more of most-trusted successors  $u_k$  of  $u_i$  that distrust  $u_j$  rather than trust  $u_j$ . In other words, for the purposes of  $u_j$ , there are more disapprovals than endorsements via  $u_i$ ’s successors.

$\forall u_i, u_j \in \text{UN}: u_i$  **can distrust**  $u_j$  if  
 $(u_i, u_j) \in \text{NTL} \vee$   
 $[$   
 $\| \{ (u_i, u_k) \in \text{PTL} \mid \mathcal{T}(u_k, u_j) = \text{false}$   
 $\wedge \neg \exists u_l \in \text{UN} : (u_k \prec_{u_i} u_l) \wedge (u_i, u_l) \in \text{PTL}$   
 $\wedge \mathcal{T}(u_l, u_j) = \text{true} \} \|$   
 is greater than  
 $\| \{ (u_i, u_k) \in \text{PTL} \mid \mathcal{T}(u_k, u_j) = \text{true}$   
 $\wedge \neg \exists u_l \in \text{UN} : (u_k \prec_{u_i} u_l) \wedge (u_i, u_l) \in \text{PTL}$   
 $\wedge \mathcal{T}(u_l, u_j) = \text{false} \} \|$   
 $]$

**Evidence in support of Belief:**  $u_i$  can believe  $s$  if there is an explicit belief link from  $u_i$  to  $s$ , or there are more of most-trusted predecessors  $u_k$  of  $s$  that  $u_i$  trusts and that believe  $s$  rather than disbelieve  $s$ . In other words, for the purposes of  $s$ , there are more affirmations than negations from  $s$ 's predecessors.

$\forall u_i \in \text{UN}, \forall s \in \text{SN}: u_i$  **can believe**  $s$  if  
 $(u_i, s) \in \text{PBL} \vee$   
 $[$   
 $\| \{ (u_k, s) \in \text{PBL} \mid \mathcal{T}(u_i, u_k) = \text{true}$   
 $\wedge \neg \exists u_l \in \text{UN} : (u_k \triangleleft_s u_l) \wedge (u_l, s) \in \text{NBL}$   
 $\wedge \mathcal{T}(u_i, u_l) = \text{true} \} \|$   
 is greater than  
 $\| \{ (u_k, s) \in \text{NBL} \mid \mathcal{T}(u_i, u_k) = \text{true}$   
 $\wedge \neg \exists u_l \in \text{UN} : (u_k \triangleleft_s u_l) \wedge (u_l, s) \in \text{PBL}$   
 $\wedge \mathcal{T}(u_i, u_l) = \text{true} \} \|$   
 $]$

**Evidence in support of Disbelief:**  $u_i$  can disbelieve  $u_j$  if there is an explicit distrust link from  $u_i$  to  $s$ , or there are more of most-trusted predecessors  $u_k$  of  $s$  that  $u_i$  trusts and that disbelieve  $s$  rather than believe  $s$ . In other words, for the purposes of  $s$ , there are more negations than affirmations from  $s$ 's predecessors.

$\forall u_i \in \text{UN}, \forall s \in \text{SN}: u_i$  **can disbelieve**  $s$  if  
 $(u_i, s) \in \text{NBL} \vee$   
 $[$   
 $\| \{ (u_k, s) \in \text{NBL} \mid \mathcal{T}(u_i, u_k) = \text{true}$   
 $\wedge \neg \exists u_l \in \text{UN} : (u_k \prec_s u_l) \wedge (u_l, s) \in \text{PBL} \wedge$   
 $\wedge \mathcal{T}(u_i, u_l) = \text{true} \}$   $\|$   
 is greater than  
 $\| \{ (u_k, s) \in \text{PBL} \mid \mathcal{T}(u_i, u_k) = \text{true}$   
 $\wedge \neg \exists u_l \in \text{UN} : (u_k \prec_s u_l) \wedge (u_l, s) \in \text{NBL}$   
 $\wedge \mathcal{T}(u_i, u_l) = \text{true} \}$   $\|$   
 $]$

### 3.2 Characteristics and Limitations of the Semantics

One can associate a unique meaning (in the form of trust and belief function) with each trust-belief DAG according to the semantics developed in Section 3.1. The trust function  $\mathcal{T}$  can be computed in one-pass starting with user nodes that have (dis)trust link out-degree of zero and processing user nodes in reverse topological order. Furthermore, only the out-links order ( $\prec$ ) associated with (dis)trust links matters. The belief function  $\mathcal{B}$  can be computed after  $\mathcal{T}$  has been determined using statement nodes and (dis)belief links. Furthermore, only in-links order ( $\triangleleft$ ) associated with (dis)belief links matters. Observe that the ordering of users with direct (dis)belief links to a statement can potentially depend on the statement. However, as specified, that order is assumed to be the same irrespective of which user is computing its belief function (making a decision). For instance, let users  $u_1$  and  $u_2$  trust  $u_3$  and  $u_4$ . Furthermore, if  $u_3$  is trusted more than  $u_4$  with respect to statement  $s_1$  and  $u_4$  is trusted more than  $u_3$  with respect to statement  $s_2$ , then  $u_1$  and  $u_2$  have similar (coupled) beliefs with respect to both  $s_1$  and  $s_2$ . (More concretely, let  $u_3$  be a cardiac surgeon,  $u_4$  be a car mechanic,  $s_1$  be a fact about coronary bypass surgery, and  $s_2$  be a fact about car's transmission.) In other words, users with direct links to statements are ordered in an "objective" manner. Note also that this approach employs counts to resolve potential conflicts only locally and propagates only boolean (binary) outcomes. (It is also possible to use percentage-based thresholds to arrive at a boolean decision.) For DAGs, the complexity of trust and belief function computation is linear in the size of the network (number of nodes and links).

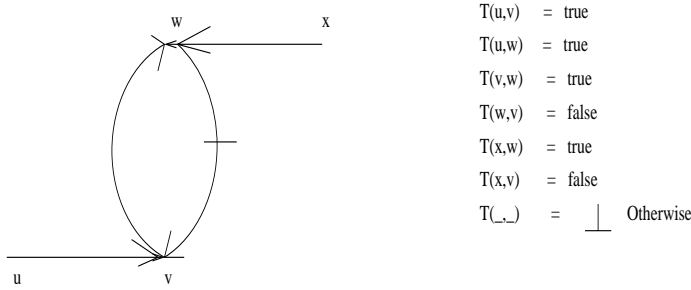


Figure 2: Cycle in General Trust-Belief Network

As explained so far, the ordering of in-links ( $\prec_s$ ) from user nodes into statement node  $s$  is a function of  $s$ -alone. This is reasonable if the predecessors of node  $s$  can be objectively rated. As a consequence, the (dis)beliefs of the various users with respect to a statement are *coupled*. However, similarly to inheritance networks [17], it is also possible to generalize this local ordering to a *ground local* ordering where the in-links order ( $\prec_s(u)$ ) depends not only on the statement  $s$  but also on the user  $u$ . This added expressive power comes with additional computational overhead. For instance, let users  $u_1$  and  $u_2$  trust  $u_3$  and  $u_4$ . Furthermore, with respect to statement  $s$ , let  $u_1$  trust  $u_3$  in preference to  $u_4$ , and while let  $u_2$  trust  $u_4$  in preference to  $u_3$ . In this case, the beliefs of  $u_1$  and  $u_2$  need not be coupled with respect to  $s$ . (More concretely, let  $u_3$  be a general physician,  $u_4$  be  $u_1$ 's father, a recovering cancer patient, and  $s$  be a fact about chemotherapy treatment.  $u_1$  may give more credence to the insights of  $u_4$ , while a bystander  $u_2$  may value the opinions of  $u_3$ .)

### 3.3 Semantics of Trust-Belief Networks: Dealing with Cycles

The semantics specification presented so far is not suitable for trust networks containing cycles that can cause apparent inconsistency or require iterative fixed point computation, in the general case. However, it is possible to associate unique semantics to the network if we can define a “personal” DAG for each user that can be used to determine trust and belief relationships for that user using the above approach. For example, consider the simple network with cycle shown in Figure 2. Even though there is a cycle, we can unambiguously conclude that user  $u$  trusts user  $v$  (resp.  $x$  trusts  $w$ ) in spite of a roundabout argument supporting  $u$  distrusts  $v$  via  $w$ .

The computation of a topological ordering of user nodes  $u$  from a given user node  $r$  is based on a breadth-first search [5] of the ordered directed graph

( $UN, PTL, NTL$ ), which is a subgraph of the trust-belief network. The nodes that are included in the personal DAG of  $r$  are all the reachable nodes found by the breath-first search procedure and the links that we include in the personal DAG of  $r$  are all the tree edges and the cross edges. Thus, only back edges are excluded from the personal DAG. This exclusion is justifiable, since back edges represent “indirect” information that is superseded by the “direct” information available from the tree edges. The search procedure is easily modified to number the nodes as they are visited by the search. This numbering gives a topological ordering.

The trust function over the user nodes with respect to the user node  $r$  can be computed using this topological order on user nodes. In fact, this computation can be carried out in parallel with respect to all user nodes. The computational complexity for trust-belief networks with cycles is *quadratic*.

## 4 Conclusions and Future Work

In this paper, we developed a framework for describing semantics of general trust and belief networks containing cycles, exploiting and adapting many evidence-based insights originally developed in the context of inheritance networks. The framework incorporates both trust and distrust in a natural fashion. Specifically, it distinguishes between direct and inferred trust, preferring direct information over possibly conflicting inferred information. It also represents ambiguity or inconsistency explicitly. It formalizes trust and belief values via partially ordered discrete values over information and truth scales, and aggregation via least-upper-bound operation. The propagation and aggregation can be carried out using local computations.

When initial trust information is available, e.g., ratings as in Amazon.com, etc., the trust information computed by our algorithms can be used in conjunction with the ranking information provided by current search engines to make informed decisions about the content (or product or seller). In future, it is necessary to augment user or certifying agency provided ratings with automatic mechanisms to seed trust judgments based on provenance information, link analysis, policies, reputation, and so forth.

As Wang and Singh [20, 21] have noted recently, there are no “standard” data sets and no benchmarks available beyond specific adaptations of the basic Epinions data set and some work by [7]. As this situation is ameliorated in the future, it will be possible to conduct some realistic experiments to illustrate our approach.

## References

- [1] Donovan Artz and Yolanda Gil. A Survey of Trust in Computer Science and the Semantic Web. *Journal of Web Semantics*. Volume 5, Issue 2. pp. 58–71, 2007.
- [2] N. D. Belnap. How a computer should think. *Contemporary Aspects of Philosophy*, G. Ryle (ed.). Oriel Press, pp. 30–56, 1977.
- [3] V. G. Bintzios, T. G. Papaioannou, and G. D. Stamoulis. An effective approach for accurate estimation of trust of distant information sources in the semantic Web Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing. 6 pages, 2006.
- [4] S. Brin and L. Page. The Anatomy of a Large-Scale Hypertextual Web Search Engine. *WWW7 / Computer Networks* 30(1-7), pp. 107-117, 1998.
- [5] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Cliff Stein. *Introduction to Algorithms (Second Edition)* MIT Press and McGraw-Hill. 2005.
- [6] [http://www.trustlet.org/wiki/Epinions\\_dataset](http://www.trustlet.org/wiki/Epinions_dataset), 2003.
- [7] Karen Fullam, Tomas B. Klos, Guillaume Muller, Jordi Sabater, Andreas Schlosser, Zvi Topol, K. Suzanne Barber, Jeffrey S. Rosenschein, Laurent Vercoeur, and Marco Voss. A specification of the Agent Reputation and Trust (ART) testbed: experimentation and competition for trust in agent societies. In *Proc. of the 4th International Joint Conference on Autonomous Agents and MultiAgent Systems*, pages 512-518. ACM Press, July 2005.
- [8] J. Golbeck and J. Hendler. Inferring Trust Relationships in Web-based Social Network. *ACM Transactions on Internet Technology*. (to appear)
- [9] R. Guha, Ravi Kumar, Prabhakar Raghavan, Andrew Tomkins. Propagation of Trust and Distrust. *International World Wide Web Conference (WWW2004)*, pp. 403–412, 2004.
- [10] Y. Katz and J. Golbeck. Social Network-based Trust in Prioritized Default Logic. *Proceedings of The Twenty-First National Conference on Artificial Intelligence (AAAI-06)*, 2006.
- [11] J. Horty, R. Thomason, and D. Touretzky. Mixing strict and defeasible inheritance. *Proceedings of the Seventh National Conference on Artificial Intelligence (AAAI-88)*, pp. 427 - 432, 1988.

- [12] J. Horty, and R. Thomason. A skeptical theory of inheritance in nonmonotonic semantic networks. *Artificial Intelligence*, Vol. 42, pp. 311 - 348, 1990.
- [13] P. Massa and C. Hayes. Page-reRank: Using Trusted Links to Re-rank Authority. *Web Intelligence Conference*, pp. 614-617, 2005.
- [14] P. Massa and P. Avesani. Trust-aware recommender systems. *Proceedings of the 2007 ACM Conference On Recommender Systems*, pp. 17-24, 2007.
- [15] M. Richardson, R. Agrawal and P. Domingos. Trust Management for the Semantic Web. *Proceedings of the Second International Semantic Web Conference*, pp. 351–368, 2003.
- [16] K. Thirunarayan and Michael Kifer. A Theory of Nonmonotonic Inheritance Based on Annotated Logic. *Artificial Intelligence Journal*, Vol. 60, pp. 23–50. March 1993.
- [17] K. Thirunarayan. Local Theories of Inheritance. *International Journal of Intelligent Systems*, Vol. 10(7), 617–645, July 1995.
- [18] K. Thirunarayan. On the Equivalence of Upward and Downward Inheritance Reasoners *Annals of Mathematics and Artificial Intelligence*, Vol. 15(2), 239–256, November 1995.
- [19] D. Touretzky, R. Thomason, and J. Horty. A skeptic’s menagerie: conflictors, preemptors, reinstaters, and zombies in nonmonotonic inheritance. *Proceedings of the Twelfth International Joint Conference on Artificial Intelligence (IJCAI-91)*, pp. 478 - 483, 1991.
- [20] Y. Wang and M.P. Singh. Trust Representation and Aggregation in a Distributed Agent System. *Proceedings of the Twenty-First National Conference on Artificial Intelligence (AAAI-06)*. 2006.
- [21] Y. Wang and M.P. Singh. Formal Trust Model for Multiagent Systems. In *Proceedings of the 20th International Joint Conference on Artificial Intelligence (IJCAI-07)*. pp. 1551 - 1556, 2007.
- [22] X. Wang, J. You, and L. Yuan. A Default Interpretation of Defeasible Network. *Proceedings of the Twelfth International Joint Conference on Artificial Intelligence (IJCAI-97)*, pp. 156 - 161, 1997.
- [23] C. N. Ziegler and G. Lausen. Propagation Models for Trust and Distrust in Social Networks. *Information Systems Frontiers*, Vol. 7:4/5, pp. 337-358, 2005.