18th International Conference on Information Fusion
Washington, DC - July 6-9, 2015

Semiring-Based Trust Evaluation for Information Fusion in Social Network Services

Peixin Gao
Dept of Electrical & Computer Eng and
Institute for Systems Research
University of Maryland
College Park, Maryland 20742
Email: gaopei@umd.edu

John S. Baras
Dept of Electrical & Computer Eng and
Institute for Systems Research
University of Maryland
College Park, Maryland 20742
Email: baras@umd.edu

Jennifer Golbeck
College of Information Studies and
Department of Computer Science
University of Maryland
College Park, Maryland 20742
Email: jgolbeck@umd.edu

***Abstract*—As online social network services (SNS) are booming and gaining tremendous popularity, there is a sharply increasing amount of information exchange and interactions among SNS users. Taking this advantage, users in SNS make decisions via collecting and combining information from different sources (i.e. other users). However, there exists a large variance of trustworthiness among SNS populations, which is threatening the quality of the information fusion process. In such circumstances, trust relationships among users in SNS are very important in decision making as well as for the success of many SNS-based applications, e.g. recommender systems and ad targeting. An appropriate trust inference mechanism for trust evaluation is necessary in extending the knowledge base of trust opinions and tackle the issue of limited trust information due to link sparsity in social networks. In this work, we model the trust relationship among users in SNS as a 2-dimensional vector, and propose a semiring-based model for trust propagation and fusion as the building block of our trust inference framework. Specifically, in our approach, both trust and distrust (i.e., positive and negative trust) are both considered, and opinion conflict resolution is supported by our framework of trust inference.**

I. Introduction

With the fast development of Internet and IT technologies, online social network services (SNS) such as Facebook and Twitter are booming and gaining tremendous popularity. Via exposing personal behaviors and connecting to each other, hundreds of millions of users interact and exchange information over these platforms [1]. The sharply increasing amount of information flowing in SNS brings a significant benefit to the users in SNS as they could make decisions via collecting and combining information from different sources (i.e. other users) in the network. Such patterns of information fusion process have opened a promising market for SNS-based applications. For example, in recommender systems, the preference of a user is predicted by users with similar taste [2], and the recommendations can be further personalized based on social connections and interactions of users in SNS [3]–[5]. Other applications like ad targeting [6] and personalized email service [7] also apply information from SNS for better performance. However, there exists a large variance of trustworthiness and preference among SNS populations, which is threatening the quality of the information fusion process. Meanwhile, based on the interactions within the social network, there is an aligned network of trust, where users in SNS have direct trust opinions about those other users and sources of information they interact with. In such circumstances, trust relationships among users in SNS are very important in decision making as well as for the success of many SNS-based applications.

However, social network connections are naturally sparse, so is the underlying trust network. Due to the scale-free nature of the user degree in social networks [8], most users only have a very small number of connections to other users in the network, compared to the size of the network. Meanwhile, however, social networks display the so-called "small-world" effect [9], i.e. there exists a relatively short path connecting most pairs of nodes within the network. Thus though each user has very limited trust information about others, most users are able to connect to others via paths within the network. This fact makes trust inference a necessary and ideal approach to tackle the problem of connection sparsity via reaching trust relationships among users with indirect connections.

Transitivity is the foundation of most trust inference models. Guha et al. [10] listed four types of trust transitivity models, namely direct propagation, co-citation, transpose trust and trust coupling. Among these four categories, direct propagation is mostly considered and can be seen as the classical transitivity. Based on the assumption of transitivity (or partial transitivity), trust information can propagate along the paths in a trust network that connect two users and trust relationship can be inferred. In our trust inference framework, we also admit trust transitivity and use direct propagation as the form of transitivity.

When considering trust inference, distrust is another component that should be considered. Distrust information can be used to differentiate unknown users from ones that are not trusted, that people of zero trust are unknown while those of negative trust (i.e. distrust) can be identified as antagonistic or opposite in opinions or preferences. However, the transitivity over distrust is much more complicated than the one associated with trust [11]. For example, it is not obvious what the trust relation between Alice and Charlie is if Alice distrusts Bob and Bob distrusts Charlie.

In this work, we propose to model the trust relationships among users in SNS as a 2-dimensional vector, in order to

present the information contained in trust relationships. In the vector, both trust level and certainty level about the trustee are considered, so that more complicated situations can be modeled and analyzed. By making trust level take values in the range of $[-1, 1]$, distrust is considered along with trust (i.e., negative and positive trust). Based on the trust network and trust vector, we develop a semiring model for trust propagation and fusion (aggregation). Our trust inference algorithm is thus designed with trust propagation and fusion, where opinion conflict resolution is supported via trust fusion.

Our contribution in this paper is two-fold:

- First, based on an appropriate interpretation of trust in social network scenarios, we introduce a 2-D trust measure for trust evaluation, where two independent factors in trust are both considered.
- Second, we propose novel metrics for trust inference based on semiring models, where both trust and distrust are both considered in our framework. Specifically, transitivity of trust and distrust are discussed and handled differently.

In the following sections, we will discuss the different application scenarios where trust mechanism applies and plays an important role, along with corresponding interpretations of trust, with an emphasis on the application of trust in social network services. We will also introduce the semiring framework as a promising mathematical tool for trust inference. We will propose our model of trust opinion, which is defined as a 2-D vector. A semiring-based trust metric is developed upon the trust network for trust inference and conflict resolution. Based on such trust metric, we further propose a trust inference algorithm via trust propagation and fusion. An example case is given to illustrate the working mechanism of the inference algorithm, followed by a discussion about the algorithm and future directions of research.

II. Preliminary

A. Trust Evaluation in SNS

The concept of trust has been widely applied in many different domains, which makes trust an umbrella term of multiple interpretations. In the Public Key Infrastructure (PKI), trust is used for authentication and secure transactions [12], [13]. In P2P networks, a global trust is evaluated to regulate the interactions among users in the network [14]. Trust is also an important concept for security in Ad Hoc Networks, influencing processes like intrusion detection and access control [15], [16]. In such application scenarios, trust can be treated as a measure of integrity or level of confidence in cooperation.

In the case of social network services (SNS), trust is interpreted in a more subjective way. Here trust is a directed relationship between users and is a compound of integrity, preference/taste similarity and social closeness, and could be defined as, in a certainty domain (area), the extent to which a truster will consider the trustee's opinions in such domain. Such a definition makes trust a domain-specific concept that is tailored for social network scenarios. A lot of research has been conducted in inferring and evaluating trust/distrust relationships in SNS, as well as establishing a trust network based on trust relationships.

Guha et al. [10] conducted one of the earliest studies that addresses both trust and distrust propagation in an algorithmic way, where four types of transitivity models are discussed. Based on the transitivity model, they consider propagation of trust and distrust in several different cases via matrix operations, and opinions are combined in a rounding fashion. They recommend a one-step distrust setting which is robust and effective.

Golbeck proposed TidalTrust [7], [17] for inferring trust relationships between people with no direct connection based on shortest trust paths between them within the trust network. The algorithm aggregates the weighted trust values between neighbors to reach indirect trust. However, it only takes into account the shortest, strongest paths, thus may loose some ratings from distant users in the trust network. In the following work [18], trust paths of different length are considered. MoleTrust [19], [20] proposed by Avesani et al. is similar to TidalTrust, but considers all raters up to a fixed maximum-depth given as an input.

Jøsang et al. [21] treated trust and distrust as two separate concepts and proposed probabilistic aggregation operators for fusion. However, these operators assume that users have equal weights (equal importance), and hence lack flexibility. DuBois et al. [22] designed a probabilistic approach to infer the trust relationship between users in social networks and applied it in network clustering. In their following work [11], they further considered distrust in the network and introduced a modified spring-embedded algorithm for trust inference.

Walter et al. [23] applied mean field analysis to reach trust information from social networks, with a consideration of trust dynamics. [24] defines trust as the personal threshold determined by the trusting party that describes the maximum utility the trusting party is willing to risk when dealing with the trusted party. Kuter et al. [25] developed the SUNNY algorithm for trust inference based on probabilistic confidence models. In [26], a 2-D trust score is proposed to distinguish trust, distrust, inconsistency and ignorance. Trust propagation is defined using norm, conorm and negator, and trust aggregation uses weighted average. Huang et al. [27] used a probabilistic soft logic framework for trust prediction.

B. Semiring Structure

Semirings are a well developed tool used in solving constraint satisfaction problems (CSPs) [28]. According to [15], [29], here we give a definition of semiring.

Definition. *Semiring:* A semiring is a tuple $\langle A, \oplus, \otimes, \mathbf{0}, \mathbf{1} \rangle$ such that

- A is a (possibly infinite) set with two special elements $\mathbf{0}, \mathbf{1} \in \mathbf{A}$
- $\oplus$, called the additive operation, is commutative and associative, with $\mathbf{0}$ as the unit element, such that

$$a \oplus b = b \oplus a$$
$$a \oplus (b \oplus c) = (a \oplus b) \oplus c$$
$$a \oplus \mathbf{0} = a = \mathbf{0} \oplus a$$
$$\forall a, b, c \in A$$

- $\otimes$, the multiplicative operation, is associative, with $\mathbf{1}$ as the unit element and $\mathbf{0}$ as absorbing element, such that

$$a \otimes b = b \otimes a$$
$$a \otimes \mathbf{1} = a = \mathbf{1} \otimes a$$
$$a \otimes \mathbf{0} = \mathbf{0} = \mathbf{0} \otimes a$$
$$\forall a, b \in A$$

- $\otimes$ distributes over $\oplus$, i.e.

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$$
$$\forall a, b, c \in A$$

A semiring $\langle A, \oplus, \otimes, \mathbf{0}, \mathbf{1} \rangle$ is called an ordered semiring if $\exists$ a partial order relation $\preceq$ that is monotone with both operators:

$$a \preceq b \text{ and } a' \preceq b' \Rightarrow a \oplus a' \preceq b \oplus b' \text{ and } a \otimes a' \preceq b \otimes b'$$

For example, the set of real numbers $\mathbb{R}$, along with the usual addition and multiplication, forms a semiring, where unit elements $\mathbf{1} = 1$ and $\mathbf{0} = 0$.

Different realizations of semirings can be designed and applied in different application scenarios. Theodorakopoulos et al. [15], [30] modeled trust opinion in an Ad Hoc network as a 2-D vector of (trust, confidence), and proposed two semiring frameworks, namely path semiring and distance semiring as trust metrics for trust evaluation. [31] uses a semiring model similar to path semiring for multi-trust evaluation within a trust network.

Most works in applying semiring models for trust evaluation take trust as a non-negative measure (e.g. with a range of $[0, 1]$). In order to accommodate negative trust values (i.e. distrust), a modification on the semiring model is needed.

III. Trust Model

The main aim in setting up trust networks is to allow agents to form trust opinions on unknown agents or sources by asking for trust opinions from acquainted agents. While trust is increasingly getting established, the use and modeling of distrust remains relatively unexplored. Although recent research works [26], [32] show an emerging interest in modeling the notion of distrust, models that take into account both trust and distrust are still scarce. Most approaches completely ignore distrust, or consider trust and distrust as opposite ends of the same continuous scale. However, there is a growing body of opinion that distrust cannot be seen as the equivalent of lack of trust [10], [33].

A. Opinion Vector

As is mentioned in Sec. II, trust is domain-specific in SNS. People hold different level of trust towards others in different domains (areas); it's common that people trust others in some domains or areas instead of others. For example, we would, in most occasions, trust a physician in her opinions on our health situation, but not the physician's ideas on trends in fashion. Here for simplicity, we first consider the single domain case.

As pointed out in [7], there are actually two types of trust, i.e. trust opinion in a person, and trust in the person's opinions/recommendations. The first part describes the opinion of the truster on trustee's quality in providing messages of integrity, which can be used in evaluating confidence on the trustee's introducing other people to establish trust relationship (i.e. certainty). The later component describes the weight that the truster puts on trustee's opinion in domain-specific decision making (i.e. trust). Based on such hypothesis, we define the trust opinion as a 2-dimensional trust vector consisting of both trust level and certainty level.

Definition. *Opinion Vector*: In our trust model, trust is defined as a 2-dimensional opinion vector from truster i towards trustee j:

$$\mathbf{O}_{ij} = (t_{ij}, c_{ij})$$

where $t_{ij} \in [-1, 1]$ is the trust level representing how much i trusts (likes)/distrusts (dislikes) the opinions (taste) of j in the current domain. $c_{ij} \in [0, 1]$ is the certainty level which shows how much i believes in the integrity of j.

Trust level $t_{ij} < 0$ corresponds to a distrust relation between truster and trustee, and that there is to some extent a disagreement/opposition in preference/taste. $t_{ij} = 1$ means "totally agree"or "like", while $t_{ij} = -1$ means "totally disagree"or "dislike". $c_{ij} = 1$ shows an extreme certainty on j's integrity.

The initial trust relationship can be established based on the information in the social network. For instance, both explicit ratings (like Epinion), or extraction from user interactions (e.g. 'like' and 'dislike') can be sources of directed trust opinions.

Note that though defining trust as a 2-D vector is similar to [15], [30], which apply trust in Ad Hoc networks, the interpretation of trust and the way trust is applied is very different. Here in a social network setting, trust is used as a measure of preference and certainty is a measure of propagation credibility, instead of a representation of identity in the Ad Hoc network case. Also, here the trust component takes values in $[-1, 1]$ where a value of -1 means opposite taste/preferences, while in [15] trust is in the range of $[0, 1]$ and a value of 0 is used to denote zero-trustworthiness.

B. Trust Network

Based on the trust relationships among people in SNS, a trust network can be established. Referring to previous work [3], [7], [10], [23], [26], [32], [33], we define the concept of trust network in SNS setting as follows.

Definition. *Trust Network:* Trust network $T(V, E)$ is a directed and weighted graph established via the graph of social connections, where V is the set of nodes (i.e. users), with $|V| = N$ denoting the size of the graph. E is the set of directed edges (i.e. trust links). $\forall$ directed edge $e_{ij} = (v_i, v_j) \in E, v_i, v_j \in V$, is a directed trust link from node v_i towards v_j, with an associated opinion vector $\mathbf{O}_{ij} = (t_{ij}, c_{ij})$, indicating the opinion of trust that node v_i holds on v_j. Trust links are

not necessarily symmetric. $N_i = \{v_j | e_{ij} \in E\}$ is the neighbor set of node v_i.

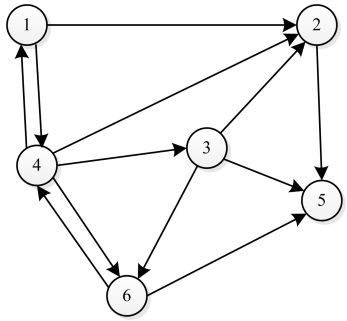

Fig. 1. An example of trust network

Fig. 1 gives an example of a trust network, where $V = \{v_1, v_2, \cdots, v_6\}$. There are 12 directed edges, each representing the trust relationship between truster (tail) and trustee (head). For node v_3, its neighbor set is $N_3 = \{v_2, v_5, v_6\}$.

C. Trust Metrics Based on Semirings

Trust networks are typically challenged by two important problems influencing trust opinions. Firstly, the trust network is naturally very sparse; in large networks it is likely that many agents do not know each other, hence there is an abundance of ignorance. Secondly, because of the lack of a central authority, different agents might provide different and even contradictory opinions, hence inconsistency may occur. In order to tackle the issue of sparse trust relationships and opinion conflict, in our trust model, we propose trust metrics based on a semiring that can handle both trust and distrust in opinion propagation and fusion (i.e. aggregation). Specifically, propagation uses a multiplication operator ($\otimes$) and fusion process is conducted via an addition operator ($\oplus$).

Based on intuitive concepts about trust establishment in the SNS setting, we can expect the addition and multiplication operators to have certain properties in addition to those defined in a general semiring structure.

Non-increasing of trust in propagation process. First of all, since an opinion should deteriorate when propagating along the trust path, the multiplicative operation which defines the process is required to satisfy:

$$\mathbf{O}_a \otimes \mathbf{O}_b \preceq \mathbf{O}_a, \mathbf{O}_b \qquad \forall \mathbf{O}_a, \mathbf{O}_b \in A$$

Non-decreasing of trust in fusion process. Regarding aggregation across multiple trust paths via additive operation, the fused opinion is expected to have better quality.

$$\mathbf{O}_a \oplus \mathbf{O}_b \succeq \mathbf{O}_a, \mathbf{O}_b \qquad \forall \mathbf{O}_a, \mathbf{O}_b \in A \text{ s.t. } sign(t_a) = sign(t_b)$$

According to our application scenario where both trust and distrust are needed to be considered in trust evaluation, we propose a novel semiring structure, which is called *distrust-semiring*.

Definition. *Distrust-Semiring:* Distrust-semiring is a tuple $\langle A, \oplus, \otimes, \mathbf{0}, \mathbf{1} \rangle$ such that

- $A = [-1, 1] \times [0, 1]$ is the set of trust opinions, with two special elements $\mathbf{0} = (0, 0), \mathbf{1} = (1, 1) \in A$
- The additive operation $\oplus$ is defined as

$$\mathbf{O}_a \oplus \mathbf{O}_b = (t, c) \tag{1}$$

where $\mathbf{O}_a = (t_a, c_a),\ \mathbf{O}_b = (t_b, c_b),\ c = max\{c_a, c_b\}$, and

$$t = \begin{cases} t_a & c_a > c_b \\ t_b & c_b > c_a \\ sign(t_a + t_b) \cdot max\{|t_a|, |t_b|\} & c_a = c_b \end{cases} \qquad \forall a, b \in A$$

- The multiplicative operation $\otimes$ is defined as

$$\mathbf{O_a} \otimes \mathbf{O_b} = (t, c) \tag{2}$$

where $c = c_a c_b$, and

$$t = \begin{cases} 0 & t_a < 0,\ t_b < 0 \\ t_a t_b & \text{otherwise} \end{cases} \qquad \forall a, b \in A$$

In the distrust semiring, the calculation of the trust component is more complex. In the additive operation ($\oplus$), it depends on the certainty level of the two opinions vectors. When the two vectors have the same certainty level, the trust level t after operation is equal to the trust level of the opinion that has the larger magnitude. This is an optimistic definition since trust opinions of higher magnitude will be selected in such setting. In the multiplicative operation ($\otimes$), if the two opinions both have negative trust values (which corresponds to distrust relationships), then the trust after operation goes to 0 meaning that the transitivity is cut in this case.

Corresponding to the distrust-semiring introduced above, we define the partial order relation '$\preceq$'.

Definition. Partial order relation $\preceq$: In distrust-semiring, for $\forall \mathbf{O}_a = (t_a, c_a)$ and $\mathbf{O}_b = (t_b, c_b) \in A$, we have

$$\mathbf{O}_a \preceq \mathbf{O}_b \tag{3}$$

if and only if

$$|t_a| \leq |t_b|$$

and

$$c_a \leq c_b.$$

Based on such a definition of the partial order relation, the distrust-semiring is a partially ordered semiring.

D. Trust Propagation

Propagation of trust opinion is based on transitivity and is defined using the $\otimes$ operator. However, the transitivity of trust and distrust are considered differently.

Definition. *Trust Propagation:* In our trust-aware system, trust opinion between two nodes s and t with no direct connection can be estimated via the multiplicative operation $\otimes$ of trust opinions of edges along the path between the two nodes.

$$\tilde{\mathbf{O}}_{st} = \prod_{\otimes, e_{ij} \in Path_{st}} \mathbf{O}_{ij} \tag{4}$$

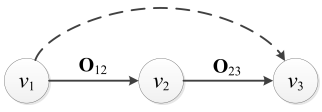

Fig. 2. Trust propagation

A maximum path length λ and trust threshold τ are set up to save computational resources and avoid infinite loops. If the path length exceeds λ or the trust value decreases below

τ along the path, then there's no trust (or distrust) relation between the two nodes.

Fig. 2 illustrates how the trust propagation works in our framework. In the example, v_1 can reach indirect trust about v_3 via its direct trust about v_2 and v_2's direct trust about v_3. If the maximum length $\lambda \geq 2$, and the threshold $\tau \leq |t_{12} \cdot t_{23}|$, then v_1's indirect trust about v_3 (i.e. $\tilde{\mathbf{O}}_{13}$) exists and it can be calculated as Eq. (5). Otherwise $\tilde{\mathbf{O}}_{13}$ doesn't exist.

$$\tilde{\mathbf{O}}_{13} = \mathbf{O}_{12} \otimes \mathbf{O}_{23} \tag{5}$$

When there are multiple paths between two nodes, the indirect trust values calculated via different paths are combined using trust fusion.

E. Trust Fusion under FATP

Trust opinion fusion across multiple paths, as mentioned above, is conducted via the $\oplus$ operator. When both aggregation and propagation appear in the trust evaluation process, there are two major ways to combine both processes together. One is called *First Aggregate Then Propagate* (FATP) and the other one is *First Propagate Then Aggregate* (FPTA). Here we apply FATP in our system.

Definition. *Trust Fusion:* Indirect trust values towards node v_t calculated from different paths can be combined in a recursive way: for nodes that have direct trust opinions about v_t, the aggregated trust values are their direct trust values; for each node v_i along the paths with no direct trust relationship with v_t, v_i learns her neighbors' trust values about v_t and combines them according to her trust towards her neighbors:

$$\tilde{\mathbf{O}}_{it} = \sum_{\oplus, v_j \in N_i, \mathbf{O}_{ij} \otimes \mathbf{O}_{jt} \succeq \sigma} \mathbf{O}_{ij} \otimes \mathbf{O}_{jt} \tag{6}$$

The opinion of neighbor $v_j \in N_i$ of v_i will not be taken into consideration if v_i has low trust level or certainty level about v_j (i.e. $|t_{ij}| < \sigma_t$ or $c_{ij} < \sigma_c$ the thresholds).

Compared to previous approaches [20], [32], such definition for trust fusion based on the $\oplus$ operator of the semiring is consistent with intuition, and can handle both trust and distrust at the same time.

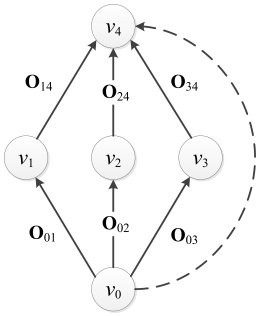

Fig. 3. Trust Fusion

Fig. 3 illustrates how the trust fusion is conducted in our system. If $\mathbf{O}_{01}$,$\mathbf{O}_{02}$ and $\mathbf{O}_{03}$ are all greater than the threshold $\sigma = (\sigma_t, \sigma_c)$, they will be considered for calculating the trust of v_0 about v_4 as shown in Eq. (7):

$$\tilde{\mathbf{O}}_{04} = (\mathbf{O}_{01} \otimes \mathbf{O}_{14}) \oplus (\mathbf{O}_{02} \otimes \mathbf{O}_{24}) \oplus (\mathbf{O}_{03} \otimes \mathbf{O}_{34}) \tag{7}$$

IV. Trust Inference Algorithm

Given a trust network and the trust model as defined in Sec. III, the trust relationship between truster (i.e. source node) and trustee (i.e. sink node) can be inferred via trust propagation and fusion using the distrust-semiring structure.

Here we propose *RingTrust*, an algorithm for trust inference in trust network $T(V, E)$ based on the distrust-semiring structure. We use $v_s \in V$ to represent the source node and $v_t \in V$ as the sink node. Let λ be the maximum trust path length, σ_t be the minimum absolute trust level, and σ_c be the minimum certainty level.

The source node $v_s \in V$ (truster) is aiming to estimate the relationship $\tilde{\mathbf{O}}_{st}$ with the sink node $v_t \in V$ (trustee), if the direct trust relationship $\mathbf{O}_{st}$ does not exist. While the maximum path length is positive ($\lambda > 0$), v_s starts from asking her neighbors, whom she has opinions at enough trust level ($t_{s\cdot} > \sigma_t$) and certainty level ($c_{s\cdot} > \sigma_c$), for their trust opinions about v_t (i.e. $\mathbf{O}_{\cdot t}$ or $\tilde{\mathbf{O}}_{\cdot t}$). Each of these neighbors, e.g. $v_i \in N_s$, provides her opinion about v_t, either direct one $\mathbf{O}_{it}$ or estimated one $\tilde{\mathbf{O}}_{it}$ calculated in the same fashion. Then v_s aggregates all the valid trust opinions to reach her opinion $\tilde{\mathbf{O}}_{st}$ about node v_t.

Here we give a recursive implementation in Alg. 1.

Algorithm 1 Trust Inference Algorithm Based on the Distrust-Semiring: **RingTrust**($v_s, v_t, \lambda, \sigma_t, \sigma_c$)

Mark v_s as visited
if $\lambda == 0$ **then**
  return $\mathbf{0} = (0, 0)$
end if
if $\mathbf{O}_{st}$ exists **then**
  return $\mathbf{O}_{st}$
end if
$\lambda = \lambda - 1$
$\tilde{\mathbf{O}} = \mathbf{0} = (0, 0)$
(**First Aggregate Then Propagate Scheme**)
for each $v_i \in N_s$, the neighbor set of node v_s **do**
  if (v_i has been visited) or ($|t_{si}| < \sigma_t$) or ($c_{si} < \sigma_c$) **then**
    continue
  end if
  $\mathbf{O}_{it} = (t_{it}, c_{it}) =$ RingTrust($v_s, v_t, \lambda, \frac{\sigma_t}{|t_{si}|}, \frac{\sigma_c}{c_{si}}$)
  if ($t_{si} < 0$, $t_{it} < 0$) or ($|t_{si} t_{it}| < \sigma_t$) or ($c_{si} c_{it} < \sigma_c$) **then**
    continue
  end if
  $\tilde{\mathbf{O}} = \tilde{\mathbf{O}} \oplus (\mathbf{O}_{si} \otimes \mathbf{O}_{it})$
end for
return $\tilde{\mathbf{O}}$

The time complexity of the algorithm is $O(N)$, with N the size of the graph. With proper settings of thresholds (e.g. λ and σ) and sampling, the efficiency of the algorithm can increase by a large scale.

By using the semiring-based trust propagation and fusion scheme, both trust and distrust (i.e. negative trust) relationships are taken into consideration for trust inference. Meanwhile, all the trust paths that are above thresholds are integrated into

the calculation, which provides better coverage and constitutes an ideal knowledge base for the algorithm to run upon. Additionally, the FATP scheme that we apply in our design has several advantages over FPTA:

- FATP has equal lengths of trust paths in aggregation at each node. For each node involved in trust evaluation, no matter the starting or intermediate ones, she only needs to aggregate information from her neighbors of direct connections (i.e. all paths have length of 2). Such feature guarantees similar credibility among paths in fusion.
- Aggregation can be treated as a low-pass filter for noise canceling and improving the opinion quality (non-decreasing property of opinion quality in trust fusion). Thus conducting aggregations at each stage of the propagation is better than operating once only at the final stage in terms of quality of inferred trust opinions.
- In the FPTA framework, for the truster to reach the inferred opinion, she needs to collect all the opinions of intermediate nodes about all related ones, which may be a threat on privacy of users not connected with the truster directly. Via FTPA, opinions of indirectly connected users are masked in the fusion process and their identities are also not disclosed to the truster. FTPA, in such aspect, can be treated as a way of privacy protection in trust evaluation.

V. Example

In order to illustrate how indirect trust relationship between users within a trust network is evaluated via *RingTrust*, we give a simple example. The part of trust network that is involved in calculating $\tilde{\mathbf{O}}_{st}$, the estimated trust opinion of v_s towards v_t, is shown as Fig. 4. Trust opinions associated with each directed edge are given. In the example, we set the following thresholds:

- Maximum trust path length $\lambda = 2$
- Minimum absolute trust level $\sigma_t = 0.2$
- Minimum certainty level $\sigma_c = 0.3$

According to the *RingTrust* algorithm discussed in Sec. IV, since v_s doesn't have direct trust opinion about v_t, she has to query her neighbors' opinions and reach an estimate, $\tilde{\mathbf{O}}_{st}$, based on these opinions. As shown in Fig. 4, v_s has six 1-hop neighbors in the trust network, v_1 to v_6, that could be used for inferring $\tilde{\mathbf{O}}_{it}$.

- Since the initial maximum path length λ is set as 2, only opinions of the neighbors who have direct trust relationship with v_t will be considered in trust fusion by v_s. Node v_1, who has no direct connection with v_t, will send an invalid opinion $\mathbf{0}$ to v_s.
- For v_2 and v_4, since they have direct trust relationship with v_t and their thresholds are satisfied, their opinion $\mathbf{O}_{2t}$ and $\mathbf{O}_{2t}$ will be sent to v_s for trust inference.
- t_{3t}, the trust level of v_3 towards v_t, is less than the threshold value $\sigma_t/|t_{s3}| = \frac{2}{3}$, thus node v_3 will reply with an invalid opinion $\mathbf{0}$ to v_s.
- The certainty level of v_s on v_5 is $c_{s5} = 0.2 < \sigma_c$, thus v_5 is not considered by v_s in calculating $\tilde{\mathbf{O}}_{st}$.

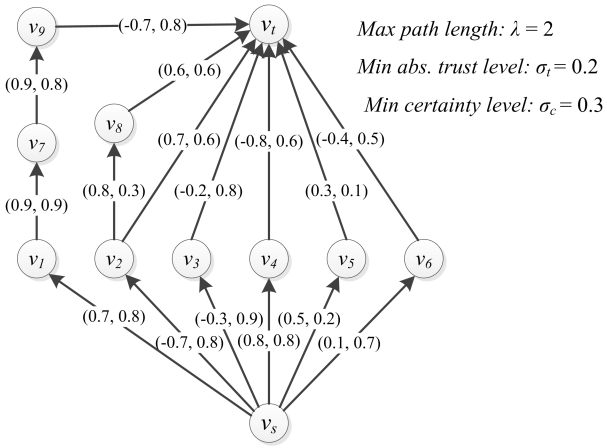

Fig. 4. Example for *RingTrust* algorithm

- v_6's opinion is not considered by v_s due to trust level $t_{s6} = 0.1 < \sigma_t$.

As as result, node v_s will calculate $\tilde{\mathbf{O}}_{st}$ by aggregating the opinions from v_2 and v_4 using $\otimes$ and $\oplus$ in distrust-semiring:

$$\begin{aligned}\tilde{\mathbf{O}}_{st} &= (\mathbf{O}_{s2} \otimes \mathbf{O}_{2t}) \oplus (\mathbf{O}_{s4} \otimes \mathbf{O}_{4t}) \\ &= ((-0.7, 0.8) \otimes (0.7, 0.6)) \oplus ((0.8, 0.8) \otimes (-0.8, 0.6)) \\ &= (-0.49, 0.48) \oplus (-0.64, 0.48) \\ &= (-0.64, 0.48)\end{aligned} \tag{8}$$

Thus the evaluated trust opinion of v_s on v_t using *RingTrust* algorithm is $\tilde{\mathbf{O}}_{st} = (-0.64, 0.48)$. As discussed in Sec. III, this result is in accordance with the properties and requirements about trust establishment in the SNS setting, including trust propagation and trust fusion.

VI. Conclusion and Future Directions

In this work, we discuss application of trust in different scenarios, especially in the social network setting. We model the trust relationships in SNS as a 2-dimensional vector, in order to denote both trust and certainty information contained in opinions. Both trust and distrust (i.e. negative trust) are considered in our model of trust. Based on the trust network and trust opinion vector, we propose a novel semiring structure, the *distrust-semiring*, for trust propagation and fusion, where operation on distrust is also supported. Specifically, transitivity of trust and distrust are handled differently. Based on the trust model and distrust semiring structure, a trust inference algorithm, *RingTrust* is developed, which evaluates indirect trust relationships via integrating trust propagation and fusion precesses in an FATP fashion. An example is given to illustrate the working mechanism of the inference algorithm. The trust information collected via this design can be used to help maintain the quality of decision making and information fusion process in SNS.

Regarding future directions, the first extension of our work resides on applying the trust inference algorithm in SNS-based applications for better quality in personalization and preference prediction. Among various applications, trust-aware social recommendation based on inferred trust relationships

will be the primary focus in our next step research [34]. As pointed out by Guha et al. [10], there are more than one possible types of transitivity within the trust network. Thus it would be another direction in our future work to consider other transitivity models in our framework of trust inference and explore their influence over the performance. In this work, the additive operation ($\oplus$) is defined for trust fusion in an optimistic way. We will evaluate other possible definitions of the operation in the semiring structure that can also resolve the opinion conflicts from different agents, and compare with our current setting. As we mentioned in this paper, trust is domain specific and people may have different trust statements (i.e. different levels of preference and certainty) about the same user within different domains, and we will investigate how trust network forms and trust inference operates in the multi-domain case, where trust would be a multi-dimensional vector. As an effect that is often ignored, delay of influence from trustees towards truster might be meaningful in tendency prediction, and we are interested in looking at such effects as well.

ACKNOWLEDGMENT

This work is partially supported by the National Security Agency, by US Air Force Office of Scientific Research MURI grant FA9550-10-1-0573, by National Science Foundation (NSF) grant CNS-1035655, and by National Institute of Standards and Technology (NIST) grant 70NANB11H148.

REFERENCES

[1] J. Ugander, B. Karrer, L. Backstrom, and C. Marlow, "The anatomy of the facebook social graph," *arXiv preprint arXiv:1111.4503*, 2011.

[2] J. L. Herlocker, J. A. Konstan, L. G. Terveen, and J. T. Riedl, "Evaluating collaborative filtering recommender systems," *ACM Transactions on Information Systems (TOIS)*, vol. 22, no. 1, pp. 5–53, 2004.

[3] P. Massa and P. Avesani, "Trust-aware recommender systems," in *Proceedings of the 2007 ACM conference on Recommender systems*. ACM, 2007, pp. 17–24.

[4] J. Golbeck, *Generating predictive movie recommendations from trust in social networks*. Springer, 2006.

[5] I. Guy, N. Zwerdling, D. Carmel, I. Ronen, E. Uziel, S. Yogev, and S. Ofek-Koifman, "Personalized recommendation of social software items based on social relations," in *Proceedings of the third ACM conference on Recommender systems*. ACM, 2009, pp. 53–60.

[6] P. Gao, H. Miao, and J. Baras, "Social network ad allocation via hyperbolic embedding," in *Decision and Control (CDC), 2014 IEEE 53rd Annual Conference on*. IEEE, Dec 2014, pp. 4875–4880.

[7] J. A. Golbeck, "Computing and applying trust in web-based social networks," 2005.

[8] A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and analysis of online social networks," in *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*. ACM, 2007, pp. 29–42.

[9] S. Milgram, "The small world problem," *Psychology today*, vol. 2, no. 1, pp. 60–67, 1967.

[10] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins, "Propagation of trust and distrust," in *Proceedings of the 13th international conference on World Wide Web*. ACM, 2004, pp. 403–412.

[11] T. DuBois, J. Golbeck, and A. Srinivasan, "Predicting trust and distrust in social networks," in *Privacy, security, risk and trust (passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom)*. IEEE, 2011, pp. 418–424.

[12] U. Maurer, "Modelling a public-key infrastructure," in *Computer SecurityESORICS 96*. Springer, 1996, pp. 325–350.

[13] P. R. Zimmermann and P. R. Zimmermann, *The official PGP user's guide*. MIT press Cambridge, 1995, vol. 265.

[14] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the 12th international conference on World Wide Web*. ACM, 2003, pp. 640–651.

[15] G. Theodorakopoulos and J. S. Baras, "Trust evaluation in ad-hoc networks," in *Proceedings of the 3rd ACM workshop on Wireless security*. ACM, 2004, pp. 1–10.

[16] J.-H. Cho, A. Swami, and R. Chen, "A survey on trust management for mobile ad hoc networks," *Communications Surveys & Tutorials, IEEE*, vol. 13, no. 4, pp. 562–583, 2011.

[17] J. Golbeck, "Personalizing applications through integration of inferred trust values in semantic web-based social networks," in *Semantic Network Analysis Workshop at the 4th International Semantic Web Conference*, vol. 16, 2005, p. 30.

[18] J. Golbeck and U. Kuter, "The ripple effect: change in trust and its impact over a social network," in *Computing with Social Trust*. Springer, 2009, pp. 169–181.

[19] P. Avesani, P. Massa, and R. Tiella, "A trust-enhanced recommender system application: Moleskiing," in *Proceedings of the 2005 ACM symposium on Applied computing*. ACM, 2005, pp. 1589–1593.

[20] P. Massa and P. Avesani, "Trust metrics on controversial users: Balancing between tyranny of the majority," *International Journal on Semantic Web and Information Systems (IJSWIS)*, vol. 3, no. 1, pp. 39–64, 2007.

[21] A. Jøsang, S. Marsh, and S. Pope, "Exploring different types of trust propagation," in *Trust management*. Springer, 2006, pp. 179–192.

[22] T. DuBois, J. Golbeck, and A. Srinivasan, "Rigorous probabilistic trust-inference with applications to clustering," in *Web Intelligence and Intelligent Agent Technologies, 2009. WI-IAT'09. IEEE/WIC/ACM International Joint Conferences on*, vol. 1. IET, 2009, pp. 655–658.

[23] F. E. Walter, S. Battiston, and F. Schweitzer, "A model of a trust-based recommendation system on a social network," *Autonomous Agents and Multi-Agent Systems*, vol. 16, no. 1, pp. 57–74, 2008.

[24] D. d. B. DeFigueiredo, E. T. Barr, and S. F. Wu, "Trust is in the eye of the beholder." in *CSE (3)*, 2009, pp. 100–108.

[25] U. Kuter and J. Golbeck, "Using probabilistic confidence models for trust inference in web-based social networks," *ACM Transactions on Internet Technology (TOIT)*, vol. 10, no. 2, p. 8, 2010.

[26] P. Victor, C. Cornelis, and M. De Cock, *Trust networks for recommender systems*. Springer, 2011, vol. 4.

[27] B. Huang, A. Kimmig, L. Getoor, and J. Golbeck, "A flexible framework for probabilistic models of social trust," in *Social Computing, Behavioral-Cultural Modeling and Prediction*. Springer, 2013, pp. 265–273.

[28] S. Bistarelli, U. Montanari, and F. Rossi, "Semiring-based constraint satisfaction and optimization," *Journal of the ACM (JACM)*, vol. 44, no. 2, pp. 201–236, 1997.

[29] S. Bistarelli, *Semirings for soft constraint solving and programming*. Springer Science & Business Media, 2004, vol. 2962.

[30] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 2, pp. 318–328, 2006.

[31] S. Bistarelli, S. N. Foley, B. O'Sullivan, and F. Santini, "Semiring-based frameworks for trust propagation in small-world networks and coalition formation criteria," *Security and Communication Networks*, vol. 3, no. 6, pp. 595–610, 2010.

[32] J. Golbeck, *Computing with social trust*. Springer, 2008.

[33] G. Gans, M. Jarke, S. Kethers, and G. Lakemeyer, "Modeling the impact of trust and distrust in agent networks," in *Proc. of AOIS01*, 2001, pp. 45–58.

[34] P. Gao, J. S. Baras, and J. Golbeck, "Trust-aware social recommender system design," in *Doctor Consortium of 2015 International Conference on Information Systems Security and Privacy*. INSTICC, 2015, pp. 19–28.