Southeast-Asian J. of Sciences: Vol.7, No 1 (2019) pp. 18-27

COMPUTATIONAL TOPIC TRUST WITH USER'S INTERESTS BASED ON PROPAGATION AND SIMILARITY MEASURE IN SOCIAL NETWORKS

Dinh Que Tran

Department of Information Technology
Post and Telecommunications Institute of Technology
Hanoi, Vietnam
email: tdque@yahoo.com

Abstract

The purpose of this work is to present a model of trust computation being defined by means of the context of user's interests and degrees of direct interaction among peers. A dynamic structure of social network based on a hierarchy of peers into k-layer neighbors w.r.t. a given source peer is investigated. We introduce a similarity measure being constructed from the space of vectors of users' interests. Up on the location of a target peer w.r.t. the hierarchy, we propose methods of estimating trust values via propagation as well as the similarity. Some classes of functions for supporting the computation of trust values in these cases are also considered.

1 Introduction

In the common life, human beings make decision based on reliability among partners in communities via connections with each others. Trust is a reliability which a peer has on his own partner for sharing knowledge or coordinating. It has been investigated from various viewpoints and the context based trust has been a increasing research topic in computer science ([4] [5] [6] [8] [10]

Key words: social networks, models of societies, text processing, decision support, distributed systems, artificial intelligence, reliability.
2010 AMS Mathematics classification: 911D30, 91D10, 68U115, 68U35, 68M14, 68M115, 68T99.

[11] [12] [14] [15]). Although discovering user's interests has attracted several researches, considering a combination of user's interests and interaction degrees among peers for estimating trust values has not been investigated strictly.

The purpose of this work is first to develop a computational trust model based on a combination of peers' interest degrees and their interaction with other peers. Second, we consider a similarity measure of users from representation in vectors of their interests. And then from a hierarchical structure with k-level neighbors of social network, we construct a computational model of trust with propagation along paths and especially with the proposed similarity for "∞-friend" peers. The contributions of our work are as follows:

- Describe a model for estimating topic trust values as a function of users interests and degrees of direct interaction among peers;
- Present the hierarchy structure of peers according to their neighbors in a directed graph for propagation computation;
- Propose a similarity measure of peers based on vectors of their interests in topics. And then construct a topic trust as a function of similar degrees and topic trust values defined via propagation.

The remainder of this paper is structured as follows. Section 2 presents some concepts and definition of a social structure based on hierarchy. Section 3 is devoted to defining topic trust and functions for estimating trust values via propagation. Section 4 presents a similarity measure based on vectors of user's interests and then investigates functions of trust computation. An algorithm for estimating topic trust values based on similarity is also described. Section 5 is conclusions.

2 Hierarchy based Social Structure

2.1 Notations

This subsection presents some definitions and notations being used in the rest of this paper.

- Each user in social media may be considered as an autonomous entity in a system. Let $\mathcal{U} = \{u_1, \ldots, u_m\}$ be a set of users or commonly called *peers*. These terms are used interchangeably in this paper. A peer needs to evaluate another peer on reliability, then the former one is called a *source peer* or *truster* and the latter one is called a *sink peer* or *trustee*;
- Let I_{ij} be a set of all *interactions* or *connections* between u_i and u_j; $\|I_{ij}\|$ be the number of such interactions. Each interaction between users u_i and u_j is a transaction at an instant time, which occurs when u_i dispatches to its wall, i.e. to u_j, a message such as post, comment, like, opinions etc;

- *Entry* is a brief piece of information dispatched from some user u_i to make a description or information/idea/opinions on an item such as a paper, a book, a film etc. We suppose that when a user is interested in some item of topic t, he is willing to dispatch an entry on it. From these entries, we can construct a classification of all them according to topics. There are various techniques for such a classification (Refer to [2] for more detail). Suppose that $\mathcal{T} = \{t_1, \cdots, t_n\}$ is a set of such topics. We denote $classifier(Entries, Topic)$ the function for classifying entries into classes.

2.2 Hierarchy Structure based on Neighbors

The section presents a concept of layer that is useful for considering propagation computation and similarity in the next section. In the following, we will formalize the concept of levels based on neighbors of peers. If u_i has some direct interaction with u_j, then u_j is called a neighbor of layer 1 or *1-layer neighbor* of u_i. We make convention that that 0-layer of u_i is u_i. The concept of *k-layer* neighbor of u_i is defined recursively as follows.

Definition 2.1. *Given a peer u_i. A peer u_j is a k-layer neighbor or k-neighbor of u_i ($k \geq 2$) iff two following conditions are satisfied:*

(i) u_j has no direct interaction from any peer of l-neighbor of u_i, for all $l \leq k - 2$

(ii) There is at least a peer of (k-1)-neighbor of u_i, which has some direct connection with u_j.

Denote L_i^k for all $k \geq 1$ to be a set of k-neighbors of u_i. It is easy to prove the following proposition.

Proposition 2.2. *Given a source peer u_i. Then there exists a number n_i such that $L_i^1 \ldots, L_i^{n_i}$ are k-neighbors of u_i and satisfy the following conditions:*

(i) For every $v \in L_i^k$ ($k = 2, \ldots, n_i$), v not being interacted directly with any one in $\cup_{l=0}^{k-2} L_i^l$.

(ii) $L_i^k \cap (\cup_{l=0}^{k-1} L_i^l) = \emptyset$, for all $k \geq 1$.

Thus, we have a taxonomy of neighbors of u_i and $L_i^1 \ldots, L_i^{n_i}$ is then called a *taxonomy* or a *hierarchy* of neighbors of u_i. Estimation of trust value of a source peer on a sink peer depends on whether the sink one belongs to taxonomy w.r.t the source. When a sink peer belonging to the hierarchy, the trust estimation on it is based on propagation. Whereas it is not of the hierarchy, computation is performed via its similarity with the other ones in some layer. A sink peer which is not of the hierarchy of a source peer is called its $\infty - friend$. We have the following definition.

Definition 2.3. *A peer u_j is called a p-friend w.r.t. a taxonomy of a source peer u_i iff $u_j \in L_i^p$ for all $p = 1, \ldots, n_i$.*

Definition 2.4. *A peer u_j is called a ∞-friend w.r.t. a taxonomy of a source peer u_i iff $u_j \notin L_i^k$ for all $k = 1, \ldots, n_i$.*

Definition 2.5. *Given two peers u_i and u_j. A path $p(i,j)$ connects two peers if there exists a sequence of peers u_k ($k = 1, \ldots, q$) having connection in couple with each others: u_i connects with u_1, u_1 connects with $u_2, \ldots, u_q$ connects with u_j. Denote $\Phi(i,j)$ be a set of all paths $p(i,j)$ connecting u_i and u_j.*

We have the following proposition.

Proposition 2.6. *Given a source peer u_i. Suppose that u_j is a p-friend of u_i. There always exists a path $p(i,j)$ connecting u_i and u_j.*

Our problem is how to estimate topic trust values in three cases: (i) There is a direct interaction among u_i and u_j; (ii) There is no any direct interaction between truster u_i and trustee u_j but there exists a path $p(i,j)$ connecting u_i and u_j; (ii) There is no path connecting u_i and u_j, it means that u_j is a ∞-friend w.r.t u_i. The detail of the topic trust model and techniques of computation based on propagation as well as similarity to deal with the problem will be presented in the next sections.

3 Modeling Trust based on Topics and Propagation Computation

This section presents an updated version of the model of topic trust and propagation functions investigated by ourselves [12].

3.1 Modeling User's Interest and Similarity

Definition 3.1. *Suppose that n_i^t is the number of entries in some topic $t \in \mathcal{T}$ a user $u_i \in \mathcal{U}$ has dispatched. Then the interest degree of u_i on topic t is defined by the following formula*

$$interest_{topic}(i,t) = \frac{1}{2}\left(\frac{n_i^t}{\sum\limits_{l \in \mathcal{T}} n_i^l} + \frac{n_i^t}{\sum\limits_{u_k \in \mathcal{U}} n_k^t}\right) \tag{3.1}$$

Thus, each peer u_i is defined as a vector of interests on various topics.

Definition 3.2. *Degrees of user's interests on all topics is defined as a vector*

$$\mathbf{u_i} = (u_i^1, \ldots, u_i^n) \tag{3.2}$$

in which u_i^k is the interest degree of user u_i in topics $t_k \in \mathcal{T}$ ($k = 1, \ldots, n$).

Definition 3.3. *Similar degree of two peers u_i and u_j is defined as a cosine similarity of two vectors $\mathbf{u_i}$ and $\mathbf{u_j}$*

$$sim(u_i, u_j) = \frac{\mathbf{u_i} \cdot \mathbf{u_j}}{\|\mathbf{u_i}\| \times \|\mathbf{u_j}\|} \tag{3.3}$$

in which $\cdot$ is the scalar product, $\times$ is the usual multiple operation and $\|\mathbf{v}\|$ is the usual length of vector.

3.2 Definition of Topic Trust

Based on direct interaction among peers, we can define trust degree among peers being named *experience trust* as follows.

Definition 3.4. *Experience trust of peer u_i on peer u_j, denoted $trust^{exp}(i, j)$, is defined by the formula*

$$trust^{exp}(i, j) = \frac{\|I_{ij}\|}{\sum_{k=1,k\neq i}^{n} \|I_{ik}\|} \tag{3.4}$$

where $\|I_{ik}\|$ is the number of connections u_i has performed with each u_k.

The problem is how to compute topic trustworthiness a source peer may rely on some sink peer in both cases with and without direct interaction.

Definition 3.5. *A topic trust a source peer u_i has on a sink peer u_j of t is a function $trust_{topic} : \mathcal{U} \times \mathcal{U} \times \mathcal{T} \to [0, 1]$, in which $[0, 1]$ is an unit interval of the real numbers. The value $trust_{topic}(i, j, t) = u_{ij}^t$ means that u_i (truster) trusts u_j (trustee) of topic t w.r.t. the degree u_{ij}^t.*

Note that the trust value u_{ij}^t depends both on interest degrees on topic t being obtained from j defined in (3.1) and experience trust degree on j computed in (3.4). It means that the topic trustworthy values are defined via a function of two variables: interest degrees and experience trust.

We now proceed to define such classes of functions, which are named *experience topic trust function* or briefly *expeto function*. Note that Definition 3.5 includes an implicit tuition that: (i) the more a peer relies on an opponent, the higher trustworthiness on some topic is; (ii) the higher interest degree of a peer on a topic t is, the more trust on him should be assigned. Thus, expeto functions must be monotonic w.r.t. two variables. We have the following definition.

Definition 3.6. *A function $f : [0, 1] \times [0, 1] \to [0, 1]$ is an experience topic trust function or expeto one iff it is monotone w.r.t. each variable.*

It is easy to prove the following proposition.

Proposition 3.7. *The following functions are expeto ones:*

(i) $f : [0,1] \times [0,1] \to [0,1]$ *is defined by the formula* $f(x,y) = x \times y$, *where* $\times$ *is the usual multiplication;*

(ii) $f : [0,1] \times [0,1] \to [0,1]$ *is defined by the formula* $f(x,y) = \mathrm{e}^{x \times y}$, *where* $\mathrm{e}^{x \times y}$ *is the usual exponential function;*

Based on the class of expeto functions, we have the following definition of experience topic trust.

Definition 3.8. *Suppose that* $trust^{exp}(i,j)$ *is the experience trust of* u_i *on* u_j *and* $interest_{topic}(j,t)$ *is the interest degree of* u_j *on the topic* t. *Then the experience topic trust of* u_i *on* u_j *of topic* t *is defined by the following formula:*

$$trust^{exp}_{topic}(i,j,t) = f_{expeto}(u^{exp}_{ij}, u^{t}_{j}) \tag{3.5}$$

where $u^{exp}_{ij} = trust^{exp}(i,j)$, $u^t_j = interest_{topic}(j,t)$ *and* $f_{expeto} : [0,1] \times [0,1] \to [0,1]$ *is an expeto function.*

3.3 Propagation based Topic Trust

Based on the taxonomy presented in Section 2, we may estimate trust values according to various paths with nodes on layers. For simplicity in presentation, we denote u_{kl} the experience topic trust value of u_k on u_l. Observe that if topic trust values of u_k on u_l and u_l on u_z are u_{kl} and u_{lz}, respectively, then trust value u_{kz} of u_k on u_z may not be higher than u_{lz} and u_{kl}. Now we proceed to construct the class of functions for estimating topic trust via propagation as follows.

Definition 3.9. *Suppose that* u_k $(k = 0, \dots, m+1)$ *is a sequence of nodes connecting* u_i *and* u_j *with convention that* $u_i = u_0$ *and* $u_j = u_{m+1}$. *A function*

$$f^{trust}_{path} : [0,1]^m \to [0,1]$$

is called path trust function, or briefly patrust, iff it satisfies the property $f^{trust}_{path}(u_{i1}, \dots, u_{mj}) \leq u_{k,k+1}$ *for all* $k = 0, \dots, m$

It is easy to prove that

Proposition 3.10. *The following functions are patrust ones:*

(i) $f(x_1, \dots, x_n) = \frac{x_1 + \cdots + x_n}{n}$

(ii) $f(x_1, \dots, x_n) = \ln(\frac{x_1 + \cdots + x_n}{n})$

(iii) $f(x_1, \dots, x_n) = \min(x_1, \dots, x_n)$

(iv) $f(x_1, \dots, x_n) = \Pi^n_{i=1} x_i$

Definition 3.11. *Suppose that $p(i,j)$ is a path with the length m connecting u_i and u_j. Topic trust of u_i on u_j along the path is defined by the following formula*

$$trust_{topic}^{p(i,j)}(u_i, u_j) = f_{path}^{trust}(u_{i1}, \dots, u_{mj}) \tag{3.6}$$

where u_{kl} are topic trust values u_k relies on u_l and $f_{path}^{trust}(p)$ is a patrust function.

In order to compute the overall topic trust from a set of paths $\Phi(i,j)$ connecting u_i and u_j, we might make use of the functions which are formalized in the following definition.

Definition 3.12. *A function $f : [0,1]^n \to [0,1]$ is a reference topic trust one iff it belongs to the following ones:*

(i) $f(x_1, \dots, x_n) = \min(x_1, \dots, x_n)$

(ii) $f(x_1, \dots, x_n) = f_{path}^{trust}(p_l)$, *where p_l is the shortest path among $p_1, \dots, p_n$*

(iii) $f(x_1, \dots, x_n) = \frac{x_1 + \cdots + x_n}{n}$

(iv) $f(x_1, \dots, x_n) = \Pi_{i=1}^n x_i$

Based on paths connecting u_i and u_j, it is able to compute topic trust value for this couple by means of the path trust functions. The trust value is then called the topic trust based on reference or briefly *reference topic trust* and denoted $trust_{topic}^{ref}(i,j,t)$. We have the following formal definition.

Definition 3.13. *Suppose that $\Phi(i,j)$ to be the set of paths $p(i,j)$ from u_i to u_j. Then the reference topic trust of u_i on u_j of t is defined by the following formula:*

$$trust_{topic}^{ref}(i,j,t) = f_{p(i,j)\in\Phi(i,j)}(trust_{topic}^{p(i,j)}(i,j,t)) \tag{3.7}$$

in which $trust_{topic}^{p(i,j)}(i,j,t) = f_{path}^{trust}(u_{i1}, \dots, u_{mj})$ is the topic trust of i on j along the path $p(i,j)$.

Based on types of topic trust functions, it is able to construct an algorithm **Algorithm 1** for computing topic trust via propagation.

4 Similarity based Topic Trust

In the previous section, we have utilized the propagation property to estimate topic trust values for nodes belonging to the corresponding hierarchy of the source node. This section is devoted to considering a method of computing trust values for ∞-friend, which is not of any level from a source node.

Algorithm 1 Computing Reference Topic Trust of u_i on u_j of topic t via class of functions

Input: The set of topics $\mathcal{T} = \{t_1, t_2, ..., t_n\}$ and the set of users $\mathcal{U} = \{u_1, u_2, ..., u_m\}$

Output: The trust of u_i on u_j of topic t, $computeRefTopicTrust^{ref}_{topic}(i, j, t)$.

$u^t_{kl} \leftarrow trust^{exp}_{topic}(k, l, t)$ //Computing experience trust for nodes with (3.5)
$\mathcal{P} \leftarrow constructTaxonomy(i)$ //constructing the set of L^k_i $(k = 1, \cdots, n)$
Define the number s such that L^s_i containing $u_j \in L^s_i$
for all t in $\mathcal{T}$ **do**
  for all $k = 1, \cdots, s-1$ **do**
    for all $u_k \in L^k_i$ **do**
      $trust^{ref}_{topic}(k-1, k, t) \leftarrow f_{p(k-1,k)} trust^{p(k-1,k)}_{topic}(k-1, k, t)$
      $trust^{ref}_{topic}(i, j, t) \leftarrow f_{p(i,j) \in \Phi(i,j)}(trust^{p(i,j)}_{topic}(i, j, t))$
    end for
  end for
end for
return $trust^{ref}_{topic}(i, j, t)$

Definition 4.1. *A function $f : [0, 1] \times [0, 1] \rightarrow [0, 1]$ is a similar topic trust function or simtrust one iff it is monotone w.r.t. each variable.*

We have the following statement.

Corollary 4.2. *If $f : [0, 1] \times [0, 1] \rightarrow [0, 1]$ is an expeto function then f is also simtrust one.*

Definition 4.3. *Given a source peer u_i. Suppose L^p_i $(p = 1, \ldots, n_i)$ is a p-level of its hierarchy and u_j is a ∞-friend. Then the similar topic trust of u_i on u_j of topic t is defined by the following formula:*

$$trust^{sim}_{topic}(u_i, u_j) = \Pi_{v \in L^p_i}(f^{trust}_{sim}(trust^{ref}_{topic}(u_i, v, t), sim(v, u_j))) \tag{4.1}$$

in which $f^{trust}_{sim}(.,.)$ is a simtrust function and Π is the usual multiplication operator.

Based on types of similar topic trust functions, it is able to construct an algorithm **Algorithm 2** for computing topic trust based on similarity.

5 Conclusions

In this paper, we introduced the computational model of topic trust based on interaction and user's interests. We described the hierarchical structure in

Algorithm 2 Computing Similarity Topic Trust of u_i on u_j of topic t via class of functions

Input: The set of topics $\mathcal{T} = \{t_1, t_2, ..., t_n\}$ and the set of users $\mathcal{U} = \{u_1, u_2, ..., u_m\}$

Output: The trust of u_i on u_j of topic t, $computeSimTopicTrust^{ref}_{topic}(i, j, t)$.

$u^t_{kl} \leftarrow trust^{exp}_{topic}(k, l, t)$ //Computing experience trust for nodes with (3.5)
$\mathcal{P} \leftarrow constructTaxonomy(i)$ //constructing the set of L^k_i $(k = 1, \cdots, n_i)$
for all t in $\mathcal{T}$ **do**
  for all $v \in L^p_i$ $(1 \leq p \leq n_i)$ **do**
    $r \leftarrow computeRefTopicTrust^{ref}_{topic}(u_i, v, t)$
    $s \leftarrow sim(v, u_j)$
    $f_v \leftarrow f^{trust}_{sim}(r, s)$
  end for
  $f \leftarrow \Pi_{v \in L^p_i}(f_v)$
end for
return $trust^{sim}_{topic}(i, j, t)$

levels of peers and constructed a similarity measure in vectors of user's interests. Methods for estimating topic trust values by means of propagation and similarity have been investigated. We also consider some classes of functions for computation in such cases. There are some open questions for further research. The first one is a comparison between topic trust values computed via propagation and similarity with various levels. Second, if topic trust estimation depends on selecting topic-trust functions and levels, restriction of computation on what levels is acceptable. We are currently performing experimental evaluation and comparison with other models on computing trust in social network. The research results will be presented in our future work.

References

[1] Wei Feng and Jianyong Wang. Incorporating heterogeneous information for personalized tag recommendation in social tagging systems. In *Proceedings of the 18th ACM SIGKDD*, KDD'12, pages 1276–1284, New York, USA, 2012.

[2] Abhishek Gattani et al. Entity extraction, linking, classification, and tagging for social media: A wikipedia-based approach. *Proc. VLDB Endow.*, 6(11):1126–1137, August 2013.

[3] Xin Li, Lei Guo, and Yihong Eric Zhao. Tag-based social interest discovery. In *Proceedings of the 17th International Conference on World Wide Web*, WWW '08, pages 675–684, New York, USA, 2008.

[4] Hideyuki Mase, Katsutoshi Kanamori, and Hayato Ohwada. Trust-aware recommender system incorporating review contents. *International Journal of Machine Learning and Computing*, 4(2), 2014.

[5] Manh Hung Nguyen and Dinh Que Tran. A combination trust model for multi-agent systems. *International Journal of Innovative Computing, Information and Control*, 9(6):2405–2420, 2013.

[6] Vedran Podobnik et al. How to calculate trust between social network users? *In 20th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 2012*, pp.1–6. IEEE, 2012.

[7] Richardson, M.; Agrawal, R.; and Domingos, Trust management for the semantic Web. *The Semantic Web: Proceedings of the 2nd International Semantic Web Conference (ISWC), volume 2870 of LNCS*, p.351368, Springer-Verlag, 2003.

[8] Wanita Sherchan, Surya Nepal, and Cecile Paris. A survey of trust in social networks. *ACM Comput. Surv.*, 45(4):47:1–47:33, August 2013.

[9] Yang Song, Lu Zhang, and C. Lee Giles. Automatic tag recommendation algorithms for social recommender systems. *ACM Trans. Web*, 5(1):4:1–4:31, February 2011.

[10] Phuong Thanh Pham, Manh Hung Nguyen and Dinh Que Tran, Incorporation of Experience and Reference-Based Topic Trust with Interests in Social Network, *Advances in Information and Communication Technology, Springer International Publishing AG 2017, M. Akagi et al. (eds.)*, pp. 1–8.

[11] Dinh Que Tran and Phuong Thanh Pham. Path Algebra for Topic Trust Computation based on References of Users in Social Network. *Southeast Asian Journal of Sciences*, 5(01), pp. 1–8, 2017.

[12] Dinh Que Tran. Classes functions for Trust Propagation in Social Network. *Southeast Asian Journal of Sciences*, 6(01), pp. 1–9, 2018.

[13] Yonghong Wang and Munindar P. Singh, Trust Representation and Aggregation in a Distributed Agent System, American Association for Artificial Intelligence, 2006.

[14] Xufei Wang, Huan Liu, and Wei Fan. Connecting users with similar interests via tag network inference. In *Proceedings of the 20th ACM International Conference on Information and Knowledge Management*, CIKM '11, pages 1019–1024, New York, NY, USA, 2011.

[15] L. Zhang, H. Fang, W. K. Ng, and J. Zhang. Intrank: Interaction ranking-based trustworthy friend recommendation. In *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, pages 266–273, Nov 2011.