Southeast-Asian J. of Sciences, Vol. 6, No. 01 (2018), pp. 1 - 9

CLASSES OF FUNCTIONS FOR PROPAGATION OF TOPIC TRUST IN SOCIAL NETWORK

Dinh Que Tran

Department of Information Technology
Posts and Telecommunications Institute of Technology (PTIT)
Hanoi, Vietnam
e-mail: tdque@yahoo.com

Abstract

The purpose of this paper is to study functions for computing topic trust in social networks. The focus is to describe classes of functions for propagation of trust among connected peers. Some of them represent properties of relationships between user's interests on topic and trust trustworthiness. Some other functions describe computational methods of topic trust values along a path and from various paths. Based on these classes of functions, we construct an algorithm for computing topic trust via propagation of topic trust among nodes.

1 Introduction

There are several models of trust computation of social networks in literature [1][4][6][7], whose approaches are based on interaction among partners or on semantics of contents from posted messages. In the recent work [6], we proposed a model of trust estimation based on interaction which is constructed from two operators concatenation and aggregation. This paper considers a more general approach of estimating topic trust values from a functional approach. The topic worthiness is a function of experience trust and user's topic interest, whereas

Key words: Computational trust, class of functions, interest, topic trust, propagation, social network.

the propagation of topic trust values is computed as a function of connection paths. It is considered as a complementary part of our previous study for a trust computing model in social network [6].

Our purpose is first to investigate properties of topic trust values via itself experience and propagation along various paths. And then we propose classes of functions for estimating topic trustworthiness based on experience evaluation and their combination from various paths.

The remainder of this paper is constructed as follows. Section 2 presents notations and basic concepts. Sections 3 and 4 are devoted to describing classes of functions for experience topic trust and propagation of trustworthiness along paths. Section 5 is conclusion.

2 Notations and Basic Concepts

In this paper, an *entry* is named for a comment, a tag, etc., which is a brief piece of information dispatched from some user u_i to make a description or post information/idea/opinions on an item such as a paper, a book, a film, a thing and so on. Assume that when a user is interested in some topic t, he is willing to dispatch entries on it. These entries may be classified into classes with respect to various topics. Several techniques have been proposed for such a classification [10][4][2][12][15]. Some necessary notations and concepts for the rest of this paper are presented as follows.

- Let $\mathcal{U} = \{u_1, \ldots, u_n\}$ be a set of users being called *universe* of users in social media. Each user may be considered as an autonomous entity in the system. Each element of $\mathcal{U}$ is also called a *peer*. A peer, who posts a message to another one, is called *source peer*; whereas the goal peer is also named *sink peer*;

- Let I_{ij} be a set of all interactions or connections between u_i and u_j and $\mid I_{ij} \mid$ 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 posts on wall or to u_j a message such as comment, like, opinions etc. Denote I_{i*} to be a set of all users with whom user i interacts.

- Let $\mathcal{T} = \{t_1, \cdots, t_n\}$ be a set of topics and denote *classifier (Entries, Topics)* to be the function for classifying entries into classes.

Definition 1. *Suppose that* n_k^t *is the number of entries a user* u_k *has dispatched in some topic* t*. Then the interest degree of* u_i *on topic* t *is defined by the* *following formula*

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

Based on interaction among peers, we can define trust degree among users that is named *experience trust* as follows.

Definition 2. *Experience trust of user u_i on user u_j, denoted $trust^{exp}(i,j)$, is defined by the formula*

$$trust^{exp}(i,j) = \frac{\|I_{ij}\|}{\sum_{k=1}^{n}\|I_{ik}\|} \quad (2)$$

$\|I_{ik}\|$ 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 when there is direct interaction and via propagation among various peers. The next sections are devoted to presenting a definition and proposing classes of functions for such a computation.

3 Classes of Functions for Experience Topic Trust

3.1 Definitions

Definition 3. *A topic trust of a source peer u_i 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 $trust_{topic}(i,j,t) = u_{ij}$ means that u_i (truster) trusts u_j (trustee) of topic t with respect to the degree u_{ij}.*

Note that the trust value u_{ij} depends on both on interest degree on topic t being obtained from j defined in (1) and experience trust degree on j computed via (2). It means that the topic trustworthiness values are defined via a function of two variables: interest degree and experience trust.

We now proceed to define classes of functions named *experience topic trust function* or briefly *expeto function*. Note that Definition 3 expresses 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 it should be assigned. Thus, an espeto function must be monotonic w.r.t. two variables. We have the following definition.

Definition 4. *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 1. *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 trust.

Definition 5. *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:*

$$trust^{exp}_{topic}(i,j,t) = f_{expeto}(u^{exp}_{ij}, \alpha_{jt}) \tag{3}$$

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

4 Functions for Computing Propagation of Topic Trust

4.1 Hierarchy of Users for Topic Trust

Our problem is how to estimate a topic trust value in the case 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.

There is then a sequence of peers u_k $(k = 1, \ldots, n)$, which have connection in couple with each others: u_i connects with u_1, u_1 connects with $u_2, \ldots, u_n$ connects with u_j. Let $\Phi(i,j)$ be a set of all paths $p(i,j)$ connecting u_i and u_j. The topic trust estimation is computed by means of middle trustees that have direct interaction with each other and defined via paths from truster u_i to trustee u_j. We observe that nodes connecting with a given node may be classified into various levels, which support trust estimation.

Definition 6. *Given peers* u_i *and* u_j*, a propagation path connecting* u_i *and* u_j *is a sequence of peers* u_k $(k = 1, \ldots, n)$ *such that* u_i *connects with* u_1*,*u_1 *connects with* $u_2, \ldots, u_n$ *connects with* u_j*.*

Definition 7. *Given a user* u_i*. A user* u_j *is 1-level neighbor of* u_i *or 1-neighbor if there is some direct interaction from* u_i *to* u_j*.*

We make convention that that 0-level of u_i is u_i. The concept of k-level neighbor of u_i is defined recursively as follows.

Definition 8. *Given a user u_i. A user u_j is a k-level neighbor or k-neighbor of u_i ($k \geq 2$), if two following conditions are satisfied:*

(i) u_j has no direct interaction from any user of l-neighbor of u_i, for all $l \leq k-1$

(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. *Given a source peer u_i. Then there is 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 connected with any one in $\cup_{l=0}^{k-1} L_i^l$.

(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 *partition* or *taxonomy* of neighbors of u_i.

4.2 Computational Propagation via Hierarchy

Based on the above taxonomy, we may estimate trust values according to various paths with nodes on levels of partition. For simplicity in presentation, we denote u_{kl} the experience topic trust value of u_k on u_l. Thus, each node u_k corresponds to a vector $\vec{u}_k = (u_{k1}, \ldots, u_{kn})$, where u_{kl} is computed with the formula (3) and $u_{kl} = \infty$ if there is no interaction among u_k and u_l.

Note 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 9. *Suppose that u_k $(k = 0, \ldots, m+1)$ 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*

$$f_{path}^{trust} : [0,1]^m \rightarrow [0,1]$$

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

It is easy to see that

Proposition 3. *The following functions are patrust ones:*

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

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

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

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

Definition 10. *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*

$$trust_{topic}^{p(i,j)}(u_i, u_j) = f_{path}^{trust}(u_{i1}, \ldots, u_{mj}) \tag{4}$$

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

Our problem is then how to compute overall topic trust from a set of paths $\Phi(i,j)$ connecting u_i and u_j. It is possible to follow one of four strategies:

- *Strategy 1:* Take minimum of all topic trust values according to paths;
- *Strategy 2:* Select the shortest path. It is based on the observation that a shorter path is more reliable;
- *Strategy 3:* It selects the most reliable neighbor with the highest trust value for going further;
- *Strategy 4:* Take mean of all paths. It is based on the fact that when there is no furthermore information, the mean is the best.

The following functions are used for estimating topic trust.

Proposition 4. *The path in which nodes appear only once in each level is the shortest path.*

We formulate them in the following definition.

Definition 11. *A function $f : [0,1]^n \to [0,1]$ is a reference topic trust one iff it belongs to the following ones:*

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

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

(iii) $f(x_1, \ldots, x_n) = \frac{x_1, \ldots, x_n}{n}$

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 topic trust based on reference or briefly *reference topic trust* and denoted $trust^{ref}_{topic}(i,j,t)$. We have the following formal definition.

Definition 12. *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:*

$$trust^{ref}_{topic}(i,j,t) = f_{p(i,j)\in\Phi(i,j)} trust^{p(i,j)}_{topic}(i,j,t) \tag{5}$$

in which $trust^{p(i,j)}_{topic}(i,j,t) = f^{trust}_{path}(u_{i1},\ldots,u_{mj})$ 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 for computing topic trust via propagation which is given in the **Algorithm 1**.

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 all nodes according to (3)
$\mathcal{P} \leftarrow constructTaxonomy(i)$ //constructing the set of L^k_i $(k = 1,\cdots,n)$
Define 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 $trust^{ref}_{topic}(i,j,t)$

Conclusions

In this paper, we have introduced a functional approach for computing topic trust. Three classes of functions have been proposed: the class of ones for computing experience trust, another one of trust along a path and the last one on composing paths. Experience trust is for direct interaction and path one is for reference trust computation to deal with the situation lacking of direct interaction among users. There are some open problems in our work. The first one is to develop further functions in class and take an evaluation. Second, whether reference topic trust estimation depends on selecting the various paths or not. The issues need to be investigated furthermore. We are currently performing experimental evaluation and comparing with other models on computing trust in social network. The research results will be presented in our future work.

References

[1] 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.

[2] Vedran Podobnik, Darko Striga, Ana Jandras, and Ignac Lovrek. How to calculate trust between social network users? In *Software, Telecommunications and Computer Networks (SoftCOM), 2012 20th International Conference on*, p.1–6. IEEE, 2012.

[3] Richardson, M.; Agrawal, R.; and Domingos, Trust management for the semantic Web. In The Semantic Web: Proceedings of the 2nd International Semantic Web Conference (ISWC), volume 2870 of LNCS, p.351368, Springer-Verlag, 2003. Available at: http://homes.cs.washington.edu/ pedrod/papers/iswc03.pdf

[4] Chung-Wei Hang et al., Operators for Propagating Trust and their Evaluation in Social Networks, Proc. of 8th Int. Conf. on Autonomous Agents and Multiagent Systems (AAMAS), 2009

[5] 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.

[6] Phuong Thanh Pham, 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.), Advances in Intelligent Systems and Computing 538, DOI 10.1007/978-3-319-49073-1 31

[7] Dinh Que Tran and Manh Hung Nguyen. Classes of trust functions for distributed intelligent computing. *Southeast Asian Journal of Sciences*, 1(2), 2012.

[8] Yonghong Wang and Munindar P. Singh, Trust Representation and Aggregation in a Distributed Agent System, American Association for Artificial Intelligence, 2006. Available at: http://www.aaai.org/Papers/AAAI/2006/AAAI06-224.pdf

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

[10] Abhishek Gattani, Digvijay S. Lamba, Nikesh Garera, Mitul Tiwari, Xiaoyong Chai, Sanjib Das, Sri Subramaniam, Anand Rajaraman, Venky Harinarayan, and AnHai Doan. Entity extraction, linking, classification, and tagging for social media: A wikipedia-based approach. *Proc. VLDB Endow.*, 6(11):1126–1137, August 2013.

[11] 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.

[12] 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, NY, USA, 2008. ACM.

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

[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. ACM.

[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.