

COMPUTATIONAL STRATEGIES FOR TOPIC TRUST PROPAGATION BASED ON K-LEVEL NEIGHBORS

Dinh Que Tran¹, Phuong Thanh Pham²

¹*Department of Information Technology
Posts and Telecommunications Institute of Technology (PTIT)
Hanoi, Vietnam*

²*Department of Mathematics and Informatics
Thang long University
Hanoi, Vietnam
E-mail: tdque@yahoo.com, ppthanh216@gmail.com*

Abstract

Topic trust in social networks is defined by means of a function of trust degrees, which are estimated via interaction experience and user interests. The computation of such a function is based on propagation of trust values along paths with neighbor nodes and thus own highly computational cost. In this paper, we first consider various strategies for estimating topic trust based on a hierarchy of users with k-level neighbors. Then we introduce algorithms for computing topic trust values w.r.t. these strategies.

1 Introduction

Trust is a reliability which a user has on his own partner in the process of its interaction. It has become crucial factor for partners to share knowledge or to coordinate in actions with each others. There are various models of

Key words: social networks, models of societies, text processing, decision support, distributed systems, artificial intelligence, reliability.

2010 AMS Mathematics classification: 91D30, 91D10, 68U115, 68U35, 68M14, 68M115, 68T99.

computational trust proposed in literature [1] [3] [5] [8] [13]. They are mainly based on interaction experience among partners and lack of considering context in which some reliability is computed. For example, a peer may rely on another one about smart phone comments rather than opinions of computer selection. In social networks, peers utilize their own entries to annotate and organize items for searching or sharing viewpoints and opinions as well. Such entries are a kind of meta-data composed of keywords or terms to introduce bookmarks, article titles, comments of items or digital images etc. They have contributed to discovering user interests for various online applications such as recommender systems, searching engine, predicting customer opinions [10] [11] [12]. In our recent work [6], the computational topic trust in the social network is estimated via a function of connections and degrees of user's interests on topics among a *truster* on a *trustee*. The problem is that such a approach has to exhaustively find all possible paths from a source truster to a sink trustee.

In this paper, we address techniques to deal with effectiveness of computation. Our approach is based on the hierarchical structure from concept of "the nearest neighbor" of nodes in a graph to classify peers into levels. Up on selecting connections of nodes among levels, we have various strategies. This work is a furthermore development of the previous one studied by ourself [7].

The remainder of this paper is structured as follows. Section 2 presents some concepts, definition and hierarchical structure and paths. Section 3 is devoted to experience topic trust which is formulated from direct interaction among peers. Section 4 describes the concept of reference topic trust based on path algebra. Section 5 presents computational strategies and corresponding algorithms. Section 6 is conclusions.

2 Hierarchical Structure and Paths

2.1 Notations and Definitions

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

- Each user in social media may be considered as an autonomous entity in the system. Let $\mathcal{U} = \{u_1, \dots, u_m\}$ be a set of users being called *universe*, whose elements are also called a *peer*. In this paper, the terms of peer and user are used interchangeably;
- When a peer estimates a topic trust value on another peer then the former one is called a *source peer* or *truster* and the latter is a *sink peer* or *trustee*.
- Let I_{ij} be a set of all interactions or connections between u_i and u_j and $\|I_{ij}\|$ 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 sends to u_j via some "wall" messages 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 post information/idea/opinions on an item such as a paper, a book, a film, a thing and so on. Suppose that when a user is interested in some topic t , he is willing to dispatch an entry on it. From such entries, we can construct a classification of them according to topics. There are many techniques for such a classification e.g. in [11]. Suppose that $\mathcal{T} = \{t_1, \dots, t_n\}$ is a set of such topics. We denote $classifier(Entries, Topic)$ the function for classifying entries into classes.

2.2 Hierarchical Structure of Peers and Paths

This subsection presents the concept of path based on hierarchical structure in levels of peers being proposed in our previous work [8]. The structure is constructed from neighbors of peers as follows. If u_i is source peer and has some direct interaction with u_j , then u_j is called a neighbor of layer 1 or *1-neighbor* of u_i . With the convention that 0-neighbor of u_i is u_i , we have a recursive definition of the concept of *k-neighbor* of u_i .

Definition 1 ([8]). *Given a peer u_i . A peer u_j is a k -neighbor of u_i ($k \geq 2$) iff two following conditions are satisfied:*

1. u_j has no direct interaction from any peer of l -neighbor of u_i , for all $l \leq k - 2$
2. 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 . We have the following proposition.

Proposition 1 ([8]). *Given a source peer u_i . Then there exists a number n_i such that $L_i^1, \dots, L_i^{n_i}$ are k -neighbors of u_i and satisfy the following conditions:*

1. For every $v \in L_i^k$ ($k = 2, \dots, n_i$), v not being interacted directly with any one in $\cup_{l=0}^{k-2} L_i^l$.
2. $L_i^k \cap (\cup_{l=0}^{k-1} L_i^l) = \emptyset$, for all $k \geq 1$.

Thus, we have a taxonomy of neighbors of u_i and $L_i^1, \dots, L_i^{n_i}$ 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. This paper focuses on considering the case in which a sink peer is included in some level. Such sink peer is called *p-friend* and its trustworthiness

is estimated via propagation. A sink peer, which is not of any level of the hierarchy, called ∞ -friend, has been considered in our work [8]. We have the following definition.

Definition 2. 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 $p = 1, \dots, n_i$.

Definition 3. Given two peers u_i and u_j . A path $p(i, j)$ connects two peers iff there exists a sequence of peers u_k ($k = 1, \dots, q$) having connection in couple with each others: u_i connects with u_1 , u_1 connects with u_2, \dots, 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. Given a source peer u_i . If u_j is a p -friend of u_i , then there always exists a path $p(i, j)$ connecting u_i and u_j .

Let $L_i^1, \dots, L_i^{n_i}$ be the taxonomy of neighbors of u_i . Suppose that u_j is a p -friend needed to estimate trustworthiness, then $u_j \in L_i^p$, where $1 \leq p \leq n_i$. Denote $L_i^{p,j}$ to be the subset of L_i^p which contains all elements connecting with u_j . Let $L_i^{p-1,j}$ be a set of peers in $(p-1)$ -neighbors L_i^{p-1} having a connection with some element in $L_i^{p,j}$. Similarly, we may define $L_i^{p-2,j}$ be a set of peers in $(s-2)$ -neighbors L_i^{p-2} having a connection with some node $v \in L_i^{p-1}$. It is easy to prove the following proposition.

Proposition 3. Given a source node u_i and a sink one u_j is its p -friend. Let $L_i^1, \dots, L_i^{n_i}$ be a taxonomy of neighbors of u_i . Then there exists a sequence $L_i^{1,j}, \dots, L_i^{p-1,j}, L_i^{p,j}$, called sublevels, satisfying the following conditions:

1. $L_i^{p,j}$ contains u_j and $L_i^{k,j} \subseteq L_i^k$, for all $k = 1, \dots, p$;
2. For every $w_k \in L_i^{k,j}$ ($k = 1, \dots, p-1$), there always exists a path connecting u_i, u_j and containing w_k .

Definition 4. A path $p(i, j)$ connecting a source node u_i and a sink node u_j is called a single path iff each sublevel $L_i^{k,j}$ ($k = 1, \dots, p$) contains only one node belonging to the path.

We have the following proposition.

Proposition 4. The single path $p(i, j)$ is the shortest path connecting u_i and u_j .

Our problem is to construct techniques for estimating topic trust values in two cases: (i) There is a direct interaction among u_i and u_j . It means that u_j is a 1-friend; (ii) There is no any direct interaction between trustor u_i and trustee u_j but there exists a path $p(i, j)$ connecting u_i and u_j . It means that u_j is p -friend, where $p \geq 2$. The detail of the topic trust model and techniques of computation based on propagation to deal with the problem will be presented in the next sections.

3 Topic Trust based on Experience

Topic trustworthiness among two peers is related to their interaction experience and the context of interests in various topics. In this section, we present an updated version of the model of estimating trusted values based on experience via interaction and users interests proposed by ourselves [6] [8]. Given a source peer u_i , we will consider two cases: (i) The first case is when a sink peer is a p-friend where $p = 1$; (ii) The second case occurs when a sink peer is a p-friend where $2 \leq p \leq n_i$. This section considers the first case by introducing a model of topic trust computation w.r.t. a sink peer of 1-friend. The second case with $p \geq 2$ will be consider in the next section..

Definition 5 ([8]). A function $trust_{topic} : \mathcal{U} \times \mathcal{U} \times \mathcal{T} \rightarrow [0, 1]$ is called a topic trust function, in which $[0, 1]$ is an unit interval of the real numbers. Given a source peer u_i , a sink peer u_j and a topic t , 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 .

Definition 6. Suppose that n_i^t is the number of entries a user u_i has dispatched in some topic t . Then the interest degree of u_i on topic t is defined by the following formula

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

Definition 7. Experience trust of user u_i on user u_j , denoted $trust^{exp}(i, j)$, is defined by the formula

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

where $\|I_{ik}\|$ is the number of connections u_i with each $u_k \in \mathcal{U}$.

Based on the degrees of interaction and of user's interests, we can define the *experience topic trust* for sink peers of 1-friend of u_i as follows.

Definition 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:

$$trust_{topic}^{exp}(i, j, t) = trust^{exp}(i, j) \times interest_{topic}(j, t) \quad (3)$$

where \times is the usual multiplication operator.

Thus values of topic trust, which source peers assign to sink peers, belong to the unit interval $[0, 1]$. The above definition implies an important fact that the more a peer believes an opponent, the more the trustworthiness on some topic is high; the higher interest degree of a peer is, the more trust on him it should be assigned. In fact, the operator \times might be replaced by some monotonic function of two parameters.

4 Reference Topic Trust based on Path Algebra

The problem is now how to estimate a topic trust value of u_i on u_j when the sink peer u_i is a p-friend of u_i where $2 \leq p \leq n_i$. And then there exists a sequence of peers u_k ($k = 1, \dots, q$) such that they have interaction in couple with each others: u_i connects with u_1, u_1 connects with u_2, \dots, u_q connects with u_j . Trust estimation is defined via these paths by means of middle trustees. The trust value is then called *reference topic trust*.

We will make use of two operators concatenation \otimes and aggregation \oplus in the path algebra for propagation computation [4]. The first one is to deal with propagating experience topic trust values along a path and the second one is used to combine trust values of various paths from a source to a sink. This section presents an application of algebraic operators on paths [4] to our context.

Definition 9. *Suppose that a path $p(i, j)$ connecting u_i and u_j is consisted of nodes $u_i = u_1, u_2, \dots, u_q = u_j$. Let $trust_{topic}^{exp}(k, l, t)$ is a topic trust value of u_k on u_l . Then topic trust value along the path $p(i, j)$ is given by the formula $trust_{topic}^{p(i,j)}(i, j, t) = \otimes_{k,l} trust_{topic}^{exp}(k, l, t)$.*

Computing topic trust value from a set of paths is given in the following formal definition.

Definition 10. *Suppose that $\Phi(i, j)$ is the set of paths $p(i, j)$ connecting u_i and u_j . Then the reference topic trust of u_i on u_j of t is defined by the following formula:*

$$trust_{topic}^{ref}(i, j, t) = \oplus_{p(i,j) \in \Phi(i,j)} trust_{topic}^{p(i,j)}(i, j, t) \quad (4)$$

in which $trust_{topic}^{p(i,j)}(i, j, t) = \otimes_{k,l} trust_{topic}^{exp}(k, l, t)$ is the reference topic trust of i on j along the path $p(i, j)$.

For various applications, it is possible to make use of the usual multiplication \times for concatenation and max or min for aggregation [4]. In this paper, we utilize the multiplication \times and max for the illustrative examples. The steps of computing reference topic trust of u_i on u_j via its neighbors with concatenation and aggregation operators are described in **Algorithm 1**.

Algorithm 1 Reference Trust of u_i on u_j of topic t

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

Output: the trust of u_i on u_j of topic t , $computeRefTrust_{topic}^{ref}(i, j, t)$

```

1:  $\Phi(i, j) \leftarrow constructPathSet(i, j)$  //the set of all paths from  $u_i$  to  $u_j$ 
2: for all  $t$  in  $\mathcal{T}$  do
3:   for all  $p(i, j) \in \Phi(i, j)$  do
4:      $trust_{topic}^{p(i,j)}(i, j, t) \leftarrow \otimes_{k, l} trust_{topic}^{exp}(k, l, t)$ 
5:      $trust_{topic}^{ref}(i, j, t) \leftarrow \oplus_{p(i,j) \in \Phi(i,j)} trust_{topic}^{p(i,j)}(i, j, t)$ 
6:   end for
7: end for
8: return  $trust_{topic}^{ref}(i, j, t)$ 

```

5 Computation Strategies and Algorithms

5.1 Problem Statement

In order to estimate reference trust values, **Algorithm 1** has to exhaustively generate all paths from a source trustor to a sink trustee. Thus, it is computationally expensive to find all paths in such a social graph. Our problem is how to reduce the number of paths so that our computation is more effective. In turn, the problem results to finding out criteria for selecting various paths which are called *strategies*.

We will utilize the hierarchical structure to construct various computing strategies. Our approach is originated from the following treatments [4]:

- The shorter paths produce better accuracy because longer chains are weaker. Thus, further nodes should contribute to trustworthiness less than the nearer ones. This observation reflexes a reality that the near neighbors are more reliable than further ones.
- The most accurate information will come from the most highly trusted neighbors. Thus, we only consider nodes with trust values being above some threshold or only concern with the nodes of highest trustworthiness.

5.2 Strategies for Computation

Given a source peer u_i and u_j is a peer on which the source one needs to estimate trustworthiness. Suppose that there exists a number $p \geq 1$ such that $u_j \in L_i^p$. The contrast case, where for all k , $k \geq 1$, $u_j \notin L_i^k$, is out of this paper. In the case $k = 1$, it means that u_i directly interact with u_j and then

$trust_{topic}(i, j, t)$ is determined by **Formula 8**. The definition of topic trust based on reference for the case $k \geq 2$ is given in **Definition 10**. This section presents computation strategies as well as improved algorithms of **Algorithm 1** for estimating trustworthiness.

5.2.1 Computational Strategies

We investigate some strategies, then describe algorithms and present illustrating examples.

- *Improved Exhaustive Strategy (ImpExauS)*: Instead of computing topic trust along all paths as in the exhaustive algorithm (ExauS) **Algorithm 1**, this strategy focuses on exhaustive computation of each level before propagating to the next level. Such computation may reduce repeating cost from a level to another. Computational Steps are given in the **Algorithm 2**.
- *Most Reliable Neighbor Strategy (MoReS)*: The strategy is similar to the depth-first search in which it selects the most reliable node for going furthermore. This strategy may reduce considerably the number of paths in computation. Steps of the strategy is given in the **Algorithm 3**.
- *Shortest Path Strategy (ShoPaS)*: The strategy ShoPaS focuses on finding out shortest paths which contain only one peer of each level. It means that they are single paths. The process of computation merely applies the operator \otimes to paths and then uses the operator \oplus for composing these paths.

5.3 Illustrating Examples

We first present an example to illustrate strategies for selecting paths in estimating trust values. Suppose that a social network has a structure as a directed graph of peers $G = (V, E)$ with the following components. The set of nodes $V = \{u_i, u_k, u_l, u_m, u_j\}$ and the set of edges with corresponding topic trust values:

$$\begin{aligned} u_i \rightarrow u_k : 0.4 & \quad u_i \rightarrow u_l : 0.6 & \quad u_i \rightarrow u_m : 0.7 & \quad u_l \rightarrow u_k : 0.4 \\ u_m \rightarrow u_k : 0.8 & \quad u_k \rightarrow u_j : 0.6 & \quad u_l \rightarrow u_j : 0.7 \end{aligned}$$

We will compute topic trust values of u_i on u_j according to the above strategies. Let $L_i^1 = \{u_k, u_l, u_m\}$ be a set of nodes directly interacting with u_i . We can compute $trust_{topic}^{ref}(i, j, t)$ based on the operator aggregation \oplus being max of various paths and the operator concatenation \times for topic trusts on one path.

1. *Strategy ExauS* (Exhaustive Strategy): This strategy exhaustively finds all possible paths: $p_1 : u_i \rightarrow u_k \rightarrow u_j$ (0.24); $p_2 : u_i \rightarrow u_l \rightarrow u_j$ (0.42);

Algorithm 2 Improved Exhaustively Computing for Topic Trust of u_i on u_j of topic t

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

Output: the trust of u_i on u_j of topic t , compute $ImpExaTrust_{topic}^{ref}(i, j, t)$.

- 1: $\mathcal{P} \leftarrow constructTaxonomy(i)$ //constructing the set of L_i^k ($k = 1, \dots, n_i$)
 - 2: Define L_i^s such that $u_j \in L_i^s$
 - 3: **for all** t in \mathcal{T} **do**
 - 4: **for all** $k = 1, \dots, s - 1$ **do**
 - 5: **for all** $u_k \in L_i^k$ **do**
 - 6: $trust_{topic}^{ref}(k - 1, k, t) \leftarrow \oplus_{p(k-1,k)} trust_{topic}^{p(k-1,k)}(k - 1, k, t)$
 - 7: $trust_{topic}^{ref}(i, j, t) \leftarrow \oplus_{p(i,j) \in \Phi(i,j)} trust_{topic}^{p(i,j)}(i, j, t)$
 - 8: **end for**
 - 9: **end for**
 - 10: **end for**
 - 11: **return** $trust_{topic}^{ref}(i, j, t)$
-

Algorithm 3 Most Reliable Node based Computing for Topic Trust of u_i on u_j of topic t

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

Output: the trust of u_i on u_j of topic t , compute $MoReN_{topic}^{ref}(i, j, t)$.

- 1: $\mathcal{P}_i \leftarrow constructTaxonomy(i)$ //constructing the set of L_i^k ($k = 1, \dots, n_i$)
 - 2: $L_i^{k,j} \leftarrow \mathcal{P}_i$, $k = 1, \dots, s$ and $u_j \in L_i^{s,j}$
 - 3: **for all** t in \mathcal{T} **do**
 - 4: **for all** $k = 1, \dots, s - 1$ **do**
 - 5: **for all** $u_l \in L_i^{k,j}$ **do**
 - 6: $u_{l,r} \leftarrow \max_{u_l \rightarrow u_r}(k, r)$
 - 7: $trust_{topic}^{ref}(k - 1, k, t) \leftarrow \oplus_{p(k-1,k)} trust_{topic}^{p(k-1,k)}(k - 1, k, t)$
 - 8: $trust_{topic}^{ref}(i, j, t) \leftarrow \oplus_{p(i,j) \in \Phi(i,j)} trust_{topic}^{p(i,j)}(i, j, t)$
 - 9: **end for**
 - 10: **end for**
 - 11: **end for**
 - 12: **return** $trust_{topic}^{ref}(i, j, t)$
-

$p_3 : u_i \rightarrow u_l \rightarrow u_k \rightarrow u_j$ (0.14); $p_4 : u_i \rightarrow u_m \rightarrow u_k \rightarrow u_j$ (0.34). Then, $trust_{topic}^{ref}(i, j, t) = \oplus(p_1, p_2, p_3, p_4) = \max(p_1, p_2, p_3, p_4) = 0.42$.

2. *Strategy ImpExauS* (Improved Exhaustive Strategy): Instead of exhaustively generating all paths, this strategy focuses exhaustive computation on each level for nodes connecting with nodes in the higher level: $p_1 : u_i \rightarrow u_k$ (0.4); $p_2 : u_i \rightarrow u_l \rightarrow u_k$ (0.24); $p_3 : u_i \rightarrow u_m \rightarrow u_k$ (0.56); then $trust_{topic}^{ref}(i, k, t) = \max(p_1, p_2, p_3) = 0.56$; Nodes u_k and u_l are selected to go further to u_j ; $p_4 : u_i \rightarrow u_k \rightarrow u_j$ ($0.56 \times 0.6 = 0.34$); $p_5 : u_i \rightarrow u_l \rightarrow u_j$ ($0.6 \times 0.7 = 0.42$). Thus, $trust_{topic}^{ref}(i, j, t) = \oplus(p_4, p_5) = \max(p_4, p_5) = 0.42$.
3. *Strategy MoReN* (the Most Reliable Neighbor Strategy): It focuses on searching for the most reliable neighbors with the highest trust values from each peer. In our social graph, u_m is the most reliable neighbor and the selected path is $p_4 : u_i \rightarrow u_m \rightarrow u_k \rightarrow u_j$ (0.34) and $trust_{topic}^{ref}(i, j, t) = 0.34$
4. *Strategy ShoPaS* (the Shortest Path Strategy): Its purpose is to search the shortest path. There are two such paths from u_i to u_j : $p_1 : u_i \rightarrow u_k \rightarrow u_j$ (0.24); $p_2 : u_i \rightarrow u_l \rightarrow u_j$ (0.42). And then $trust_{topic}^{ref}(i, j, t) = \max(p_1, p_2) = 0.42$.

6 Conclusions

In this paper, we have introduced an updated version of hierarchical structure of neighbors with sub-levels and paths. From the hierarchy, we investigate strategies with the expectation to reduce computational complexity. These problems should be studied furthermore both on their effectiveness and application implementation. We are currently performing experimental evaluation and comparing with other models on trust propagation 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] Dinh Que Tran. Computational Trust Topic with user's interests based on Propagation and Similarity measure in Social Networks. To appear in *East-West J. of Mathematics*, 2019.
- [3] Vedran Podobnik et al. How to calculate trust between social network users? In *Software, Telecommunications and Computer Networks (SoftCOM), 20th International Conference on*, p.1–6. IEEE, 2012.

- [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 Intelligent Systems and Computing* 538, Springer, 2017, M. Akagi et al. (eds.).
- [7] Dinh Que Tran, Phuong Thanh Pham, Path Algebra for topic trust computation based on references of users on social networks, *Southeast-Asian J. of Sciences* Vol. 5, No. 1 (2017) pp. 1-8.
- [8] Dinh Que Tran. Classes of functions for topic trust propagation in social network. *Southeast Asian Journal of Sciences*, 6(2), 2018.
- [9] Yonghong Wang and Munindar P. Singh, Trust Representation and Aggregation in a Distributed Agent System, American Association for Artificial Intelligence, 2006.
- [10] Wei Feng and Jianyong Wang. Incorporating heterogeneous information for personalized tag recommendation in social tagging systems. In *Proceedings of the 18th KDD*, pages 1276–1284, NY, USA, 2012.
- [11] 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.
- [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.