Contents lists available at ScienceDirect

Knowledge-Based Systems

journal homepage: www.elsevier.com/locate/knosys

A topic-sensitive trust evaluation approach for users in online communities[☆]

Xu Chen [a,*], Yuyu Yuan [a], Mehmet Ali Orgun [b], Lilei Lu [a,c]

[a] *Key Laboratory of Trustworthy Distributed Computing and Service, Ministry of Education, School of Software, Beijing University of Posts and Telecommunications, Beijing, 100876, China*
[b] *Department of Computing, Macquarie University, NSW, 2109, Australia*
[c] *Department of Computer Science, Tangshan Normal University, Tangshan, Hebei 063000, China*

ARTICLE INFO

Article history:
Received 30 June 2019
Received in revised form 14 December 2019
Accepted 20 January 2020
Available online xxxx

Keywords:
Topic-sensitive analysis
Trust evaluation
Trust propagation
Context-dependency
Labeled LDA

ABSTRACT

In order to facilitate human decision making, trust evaluation has received widespread attention in many fields, especially for online services. Most of the existing methods consider trust in a person as a value which does not vary across different scenarios without any attention to the distinction of domains or communities where trust is derived. However, the notion of context is a significant and indispensable factor for trust evaluation in practice. Due to the lack of the consideration of context, traditional methods cannot resolve the issue that arises when a highly trustworthy person in one domain is likely to dominate the results of trust assessment in others where the person is in fact less authoritative. To solve this problem, in this paper, we develop a general approach to accomplish topic-sensitive trust evaluation by considering the context of trust. We first propose a general framework which presents the well-organized architecture of topic-sensitive trust evaluation in online communities. Then, a user-topic model is proposed to automatically extract topic data from user-generated content based on the Labeled Latent Dirichlet Allocation (LLDA) model. To compare the topic differences between users, we design a topic coverage function for revealing their trust relationships in diverse topics. Moreover, we employ two traditional methods and extend them to accomplish trust prediction for people with multiple domain knowledge. Experiments based on a real-world dataset show that extended topic-sensitive approaches are more adaptive and accurate than those topic-free trust evaluation approaches, especially when the trust application scenario features multiple topics.

1. Introduction

With the fast development of networking infrastructure, there is a rapid growth of users joining online communities along with an enormous amount of information distributed through the Internet daily [1]. Individuals may participate in online communities with the expectation of sharing information in a reliable and secure environment, but unfortunately, they are often exposed to a wide variety of risks and uncertainty due to the openness and large scale of online services [2]. Participants are often required to interact with strangers in online communities, with whom they have no face-to-face communication and prior knowledge. To alleviate the uncertainty of such interactions and to determine the trustworthiness of an unknown participant, trust evaluation becomes a necessary and significant tool to assist people's decision making [2,3].

One common approach to maintain trust in a large-scale system is to build a web of trust that allows users to express their trust opinions explicitly toward others [4]. However, it is rarely possible for individuals to establish direct trust relationships with everyone on the system since they typically have no prior knowledge or interaction with a majority of users online. Therefore, methods inspired by incomplete transitivity of trust [5], known as trust propagation, are proposed to find out whether an individual can trust an unknown person or not by aggregating and analyzing the information possessed by his reliable acquaintances [4,6–8]. Those methods usually maintain the web of trust based on graph theory, some of which keep the entire trust relationships between involved users, while others modify the original link structure according to their predefined rules [9]. A significant limitation of these approaches is that they ignore the distinction of various

[☆] No author associated with this paper has disclosed any potential or pertinent conflicts which may be perceived to have impending conflict with this work. For full disclosure statements refer to https://doi.org/10.1016/j.knosys.2020.105546.

[*] Corresponding author.
E-mail addresses: cx99@bupt.edu.cn (X. Chen), yuanyuyu@bupt.edu.cn (Y. Yuan), mehmet.orgun@mq.edu.au (M.A. Orgun), lilei_lu2013@163.com (L. Lu).

https://doi.org/10.1016/j.knosys.2020.105546
0950-7051/© 2020 Elsevier B.V. All rights reserved.

application scenarios from which trust is derived, and consider trust as an invariable value for a person across all domains. Prior research shows that trust is topic-dependent, also known as context-specific, as humans have different domain knowledge and expertise in different fields [10,11]. For example, an expert in computer science is unlikely to be an excellent surgeon. He may be considered highly trustworthy when the topic falls in computer science, but when someone wants to inquire about problems of cancer treatment, his words can hardly be trusted due to the lack of professional medical knowledge. This phenomenon is pretty common in reality, but it is not taken seriously in most research, which inevitably makes it more possible for a person who is highly trustworthy in one field to dominate the results of trust evaluation in other areas in which he is less authoritative actually.

Some researchers have realized this issue and started to exploit the context in which trust is derived, and have proposed several context-aware trust approaches [12–15]. Although contextual information is an essential factor for these methods, there is no effective strategy offered to collect and gain this kind of data automatically. Usually, they directly use the tags of users' transactions given by service providers as topic information to achieve the goal of being context-aware [12,13]. However, this approach is not practical in most occasions as this information is not always explicitly available. Besides, these methods do not delve deep into the notion of context itself. Since a person's professional background is not always related to the products he bought or services he received, the context information used in these methods is not necessarily the real source of topic data.

To address this issue, in this paper, we propose a general approach to accomplish topic-sensitive trust evaluation by analyzing the real source of data that harbors the topic information. We first propose a general framework to iron out a well-organized architecture of topic-sensitive trust analysis. The main thrust of the proposed approach is to develop an effective algorithm to automatically distill user topic-related information from the user-generated content in online communities based on a typical topic modeling method: the Labeled Latent Dirichlet Allocation (LLDA) model. The user-generated content is a kind of products of individual wisdom, which implicitly contains users' domain knowledge and reveals their reliability in various topics. Furthermore, we design a topic coverage function to process the topic data and discover the topic-related relationships among individuals. According to these relationships, topic differences between users are uncovered to support trust analysis further. In order to evaluate the topic-sensitive method, we employ two traditional trust propagation approaches as baselines and compare the performance of their extended versions after integrating with the proposed approach.

The main contributions of this work are outlined as follows:

- We propose a general framework to systematically organize the architecture of topic-sensitive trust evaluation, including the modules of data collection and storage, topic extraction, and trust assessment.
- We develop a user-topic model based on LLDA to automatically discover the topics in which users have expertise by analyzing the content they have generated in online communities.
- We formulate a topic coverage function to measure the coverage rate of topics between users, which makes it possible to reveal and quantify the topic relevance among users.
- We employ two traditional trust propagation approaches (i.e., TrustRank [16] and Appleseed [6]) and extend them to be sensitive toward different topics utilizing the proposed approach. These two methods also show two different ways to integrate the topic-sensitive approach into those traditional trust evaluation methods.
- We summarize the key procedures of applying the proposed method to extend topic-free trust evaluation, which are suitable for most of the conventional trust propagation approaches.

Our work fills the gaps of context-dependent trust analysis, which has not been studied extensively in existing research. We conduct experiments on a real-world dataset obtained from Stack Exchange,[1] and the results show that the extended methods outperform the existing topic-insensitive trust propagation methods in both the ranking consistency and the trust evaluation accuracy.

The remainder of this paper is organized as follows: Section 2 introduces the related works on trust evaluation and topic modeling. Section 3 demonstrates the architecture of the topic-sensitive framework and discusses the details of building the user-topic model. Section 4 shows how to implement the proposed approach to extend two topic-free trust propagation methods, and presents the key steps of this extension. Experimental results and analysis are presented in Section 5. Finally, the conclusion and future works are discussed in Section 6.

2. Related works

Our work concerns both topic analysis and trust evaluation. Therefore, we review the related works on trust models and topic extraction methods in this section.

2.1. Trust propagation models

Trust evaluation has been widely studied in computer science [5,10,11,17], and many algorithms have been proposed, among which propagative trust models are the mainstream [9]. Incomplete transitivity [5] is one of the critical properties of trust that supports trust diffusing through a network and derives new trust relationships from known ones. Jøsang et al. [18,19] defined the conditions in detail, under which trust can be partially transitive, as the theoretical basis of trust propagation. By leveraging this basis, researchers have proposed various algorithms that utilize trust propagation to facilitate trust evaluation in diverse applications. Existing propagation methods are mostly based on graph theory, which can be divided into two categories: simplification-based and analogy-based approaches [10].

2.1.1. Graph simplification-based methods

Graph simplification-based methods simplify the structure of original networks and use only a part of trust paths in graphs according to some predefined rules. For example, Golbeck [20] proposed TidalTrust to calculate the degree of trust a user can receive from others by finding the shortest and most reliable trust paths between them in social networks. Avsani et al. [21] presented a trust-enhanced approach to filter the personalized trustworthy information for users in recommendation systems by discovering the shortest trust paths from a trustor to trustees and limiting the maximum length of indirect trust paths. Wang and Wu [22] built a personalized model for users who can customize the strategy used in the trust evaluation system from multiple dimensions depending on their personal preference. Jiang et al. [23,24] designed a trust evaluation framework, SWTrust, to generate small trust graphs for the large-scale social networks by applying the small-world characteristics. Liu et al. proposed two novel algorithms called MONTE_K [25] and MFPB-HOSTP [26] to find the optimal trust paths in complex social networks under the concept of Quality of Trust. The density of networks is an important factor that decides the outcome of trust propagation approaches.

[1] https://stackexchange.com

When a social network is too sparse, it is hardly successful in finding reliable paths between two users. Kim [27] integrated a homophily-based trust network with an expertise-based trust network to ensure the density of a trust graph can meet the requirement of trust propagation approaches. By using the uninorm trust propagation operator over four-tuple information (i.e., trust, distrust, hesitancy, and inconsistency), Wu et al. [7] proposed a novel model to build the indirect trust relationships between individuals and calculate their trust weights in social networks for group decision making. For these two methods, when there is more than one indirect path between a source node and its targets, paths with the shortest length and the highest strength will be selected [28]. Based on learning automata algorithms, Ghavipour and Meybodi [8] proposed DLATrust to predict trust values between two individuals who do not have a direct connection in social networks. Only the most reliable paths to the target user are selected, where a collaborative-filtering-based strategy is used to aggregate trust in those paths for obtaining the final trust value.

2.1.2. Graph analogy-based methods

The crux of simplification-based methods is to find an effective strategy to reduce redundant trust paths and aggregate trust values from those paths. However, the impact of information loss caused by modifying the original networks is still not clear. Therefore, graph analogy-based approaches have been developed, which keep the complete structure of trust graphs without removing any nodes or edges [10]. By improving the random surfer model used in the PageRank algorithm [29], Gyöngyi et al. [16] proposed a semi-automatic algorithm, TrustRank, to detect web spam, which first manually evaluates the trustworthiness of a small set of seeds, and then discovers other trustworthy pages connecting to those reliable seeds by analyzing their link structures. Appleseed is a trust evaluation method designed by Ziegler and Lausen [6] that attempts to rank people in a reasonable order according to their trust values. They were inspired by the spreading activation models in psychology and utilized energy flows to simulate trust propagation through networks. Based on network flow theory, Wang and Wu [30] presented a novel method called FlowTrust that estimates the maximum amount of trust flowing through a trust graph. GFTrust [31] is another approach inspired by analyzing the similarity between trust propagation and network flows, which utilizes a generalized network flow problem to handle the trust path overlap and trust decay in the evaluation process. Jang et al. [32] proposed a new method, called PIN-TRUST, to compute the user trust scores using belief propagation in the process of trust evaluation, in which three types of interactions between users are defined as well, including explicit trust, implicit trust, and explicit distrust. By updating the DLATrust, Ghavipour and Meybodi [33] proposed a dynamic trust propagation approach called DyTrust to evaluate time-varying trust between indirectly connected users. Different from DLATrust that only utilizes the most reliable paths from the source user to the target user, DyTrust adopts trust opinions from all the direct neighbors of the target user.

2.2. Context-aware trust evaluation methods

The methods mentioned above make full use of the propagative nature of trust. However, not paying attention to the context-dependency is one of their significant shortcomings. Trust is topic-dependent as humans have different professional backgrounds in different domains [10]. For instance, an expert in computer science may not be an excellent surgeon, or an outstanding economist, as his educational background and work experience mainly focus on those fields related to computer science. Therefore, investigations on the given context of trust help avoid the possibility that a highly trustworthy person in one domain influences people's trust opinions toward him for other fields, where in fact, he is not truly reliable. Some researchers have tried to study the context of trust. Since TrustRank cannot recognize the different topics on the Web, Wu et al. [34] selected different seeds set for distinct topics and calculated trust scores separately for each topic. Then, these trust scores would be aggregated together as the final scores to support trust ranking. The topic information used in this method is from the Open Directory Project (ODP), which classifies the online websites into several different categories. Wang et al. [13] proposed SocialTrust approach to infer trust of participants in social networks, which builds a contextual social network structure by taking into account the social context and interaction context. Khani et al. [12] proposed a contextual trust evaluation model to recognize the trustworthy service providers for different transactions by classifying the Social Internet of Things (SIoT) environment according to the status, environment, and types of tasks for different devices. Jiang et al. [14] extracted a domain-aware trust network from the initial network by modeling trust relationships into a heterogeneous trust network and evaluating user influence in different domains. The contextual information used in these three methods is from the service records which explicitly provide the details about the type of each transaction or the category of each product.

These context-aware methods attempt to find an effective way to handle the context-dependent property of trust, but they do not offer a deep analysis of the context itself. Instead of designing a strategy to collect and analyze the involved context and topics, they reuse the contextual information explicitly provided in transactions. However, contextual information is not always explicitly available, in particular, when the trust application scenarios are not related to sales or purchases. In most cases, the real domain knowledge of a person may not be about the products he bought or the services he received, but it is the information hidden in the words he said and the articles he wrote. The user-generated content implicitly contains essential data of users, which deserves an in-depth analysis. Besides, the contextual information used in these methods can only indicate whether a topic is related to a user, but it cannot disclose how relevant the user is to the topic. So a method is required to assist context-aware trust evaluation in extracting user topics and quantifying the topic relevance between users.

2.3. Topic extraction methods

In order to analyze the user-generated content to acquire the real topic information of users, an effective topic extraction method is required. Many studies have been proposed to distill topics from texts and documents.

Term Frequency–Inverse Document Frequency (TF–IDF) [35] is a statistical method used to calculate the frequency of terms in a text for determining how important a word is to describe a document in a corpus. Two factors are employed in TF–IDF, one of which is term frequency (TF) for counting and weighting the number of times that a word occurs in a document, and the other is inverse document frequency (IDF) used to reduce the impact of frequently occurring words in the document and increase the weights of rarely occurring terms. Due to the excessive concerns on low-frequency words, TF–IDF often yields poor results on many occasions. One of the significant drawbacks of TF–IDF is that extra cluster methods and similarity calculations are usually required to assist the generation of topics as no cluster approach is offered by TF–IDF. In order to yield a relatively good result, it is necessary for TF–IDF to be combined with other approaches. For example, Zhang et al. [36] proposed a topic analysis method based

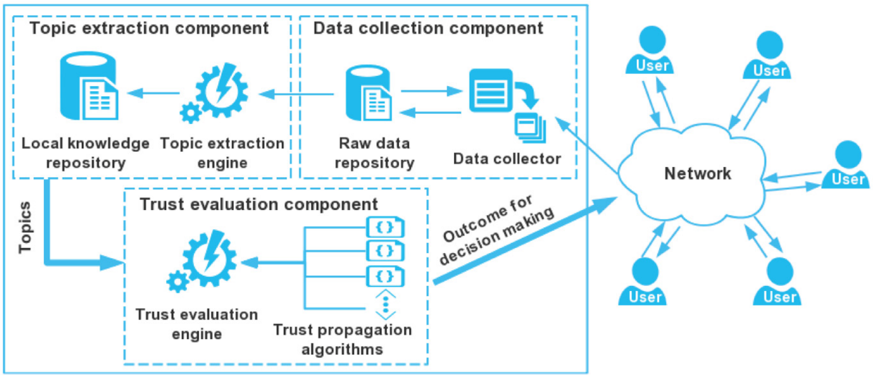

Topic extraction component
Data collection component
Local knowledge repository
Topic extraction engine
Raw data repository
Data collector
Topics
Trust evaluation component
Trust evaluation engine
Trust propagation algorithms
Outcome for decision making
Network
User
User
User
User
User

Fig. 1. The architecture of the topic-sensitive trust framework.

on a k-means clustering approach to predict the topic changes in the science field. In their work, TF–IDF was employed to preprocess the data and forecast the topic changes in the future, which produced promising results. Ghiasi et al. [37] combined the k-means algorithm and Jaccard function to find a similar context for transactions and evaluate the reputation of users in e-commerce. Worse still, the analysis offered by TF–IDF is processed at the level of words, which cannot be extended to delve into the level of topics. TF–IDF assumes that each term only has one meaning, whereas words usually have distinct meanings in different usages along with various combinations of other words. For example, consider the phrases “the sandwich is wrapped in aluminum foil” and “the role of a dramatic foil is important”. The latter sentence has nothing to do with the topic of cooking, although “foil” is commonly associated with household applications in many different scenarios. Therefore, instead of counting terms individually, text analysis methods are required to capture the real meanings of words in the context of human natural language.

To better analyze potential topics in documents, probabilistic topic models are proposed with the capability of truly delving into the semantic level of texts. Among those models, Latent Dirichlet Allocation (LDA) based methods are the most popular ones. LDA is a generative model proposed by Blei et al. [38,39] trying to automatically capture the themes hidden in an extensive collection of documents. In topic models, a topic is defined as a distribution over a fixed vocabulary, and a document can exhibit multiple topics. LDA integrates cluster analysis and latent semantic analysis methods into its algorithm. LDA is better than those conventional cluster methods, such as k-means or hierarchical clustering, which can assign only one topic to one document. Moreover, LDA employs Bayesian techniques to determine the probability of a document associated with different topics, which helps improve the accuracy of topic prediction, especially when the size of the processed data is large. Due to the advantages of LDA, it has been widely studied and applied in research. Zhou et al. [40] proposed a probabilistic model based on LDA to find the experts associated with different knowledge domains. Yau et al. [41] evaluated the performance of LDA and its extended methods according to the clustering results of academic papers in the same domain. Zhang et al. [42] detected the topic changes of the journal of Knowledge-Based Systems over the past 26 years and predicted its future trends by combining LDA and the scientific evolutionary pathway model. As an unsupervised text analysis method, LDA does not provide tools to adjust the derived topics, which often causes the difficulty of interpretation in topic clusters. To address this problem, Ramage et al. [43] extended the traditional LDA to incorporate the available tags into its learning process and improved the interpretability of topics over LDA. This approach, known as LLDA, is the base of our user-topic model. The details and reasons for choosing this method are discussed in the next section.

Based on the above investigations and analysis from different perspectives, we propose a topic-sensitive approach to extend the traditional trust propagation methods. This approach can automatically extract the topic information from user-generated data, and reveal the degree of relevance of users and their topics of interest. Our work fills the gaps of context-dependent trust analysis, which is a significant component of trust evaluation but it has not been studied extensively in existing research.

3. The topic-sensitive framework

In this section, we first describe the overall architecture of the topic-sensitive framework for trust evaluation in a networked environment. Then we present the details of how to build a user-topic model using a well-known topic modeling method: LLDA [43]. It is worth noting that topic-sensitive analysis aims to address the context-dependent issues in trust evaluation. Usually, the term context generally refers to the environment where the relationships or operations exist. However, when it comes to the nature of trust, the meaning of context is similar with that of topic, which is discussed in the scope of human knowledge and expertise for different people on diverse domains [10,11].

3.1. *Architecture of the topic-sensitive trust framework*

Fig. 1 depicts the architecture of our proposed topic-sensitive trust framework for online social networks. The framework consists of three essential components, namely, the data collection component, the topic extraction component, and the trust evaluation component.

The data collection component is used to collect the user-generated data, such as their profiles, articles, and so on. Then, these unprocessed data, which contain the underlying interests of topics of their owners, will be sent and stored in the raw data repository. Except for the function of storage, the raw data repository exchanges information with the data collector and sends data to the topic extraction engine for further analysis. The topic extraction component is the core module to manage the topic information of users, which receives the data from the collection component and prepares topic information for the trust evaluation component. The topic extraction engine is responsible for distilling the latent topics from the received unprocessed data, and then sending them to the local storage which will record these data in a local knowledge database for trust assessment. The function of the trust evaluation component is to implement trust prediction by choosing one or several practical trust analysis algorithms and extending them to be sensitive toward topics.

To the best of our knowledge, no existing study has yet proposed a complete framework for traditional trust evaluation, but Jiang et al. [10] have summarized the integrated process of trust evaluation in networked environments. We consider that process as the prototype of the traditional trust evaluation framework. In that framework, only the modules for information collection and trust evaluation are included, while in our framework, we design a module specially for extracting topics from the user-generated content. After being handled by the topic extraction engine, topic-related data will be distilled and stored in the local knowledge database for future use, or transformed into a computable form and integrated into the traditional methods to make them aware of various topics. The proposed framework forms a complete architecture of trust evaluation that includes both the traditional trust evaluation and context analysis components, and fills the gaps of context-dependent trust analysis which has been neglected by other research [4,6,16]. When trust evaluation is done appropriately, the trust inference results of our framework can be forwarded to users in the network to facilitate their decision-making process in various application scenarios.

3.2. Construction of the user-topic model

Compared with the traditional trust evaluation approaches, the topic-sensitive trust evaluation approaches put more effort into analyzing the topic-related information. This part of the work is fulfilled by the topic extraction engine, where we build a user-topic model aiming to automatically recognize the topics where users have knowledge based on those archives created by themselves. In this paper, we adopt LLDA to automate topic discovery from a large-scale collection of user-generated content.

3.2.1. The user-topic model based on LLDA

LLDA is a supervised probabilistic graphical model proposed by Ramage et al. [43] to uncover the process of labeled document generation, which considers each user-generated content as a mixture of latent topics. In topic models, a topic is formally defined as a distribution over a fixed vocabulary, and each text created by a user is a bag of words chosen from this vocabulary and simplified as a vector of words [38]. A text can have one topic or multiple topics, depending on the words it selects. Different from the unsupervised topic model: LDA [38] which does not know the range of topics in advance, LLDA constrains the model to use only those topics belonging to the observed label set.

There are three reasons for selecting LLDA as the fundamental approach for building the user-topic model in our framework. First, as a graphical model in the LDA family, LLDA has an extendable capability to be further developed and utilized in various applications. This capability makes it easy to integrate LLDA into the trust evaluation process. Second, LLDA supports the incorporation of the prior labels or tags into its learning process, which can offer a decent improvement over the traditional methods, as shown in [43]. In addition, a well-designed tool, known as the Stanford Topic Modeling Toolbox (TMT),[2] is available to support the algorithm implementation officially developed by the authors of LLDA from the Stanford Natural Language Processing Group. This tool facilitates the topic analysis on a large collection of documents. Due to these advantages, we build our user-topic model based on LLDA.

Fig. 2 illustrates the user-topic model we design based on LLDA. Here, the shaded nodes represent those observed variables, and an arrow between nodes indicates a conditional dependency between them. Compared to the original LLDA, we make two modifications in this model. One is that we introduce a user-related variable into the model by considering the relationships between users and their corresponding content. After this change, the user topic distributions can be easily obtained. The other modification is that we change the text process method according to the quality of the available data. Sometimes, a text is quite short, and it cannot accurately disclose the underlying topics in it. To ensure that the documents of users are long enough for further analysis, we aggregate all the texts generated by the same user together into a single document d. Both the changes transform the document-oriented LLDA-based model into a user-oriented topic model, which make it possible to use LLDA to analyze the user topic features.

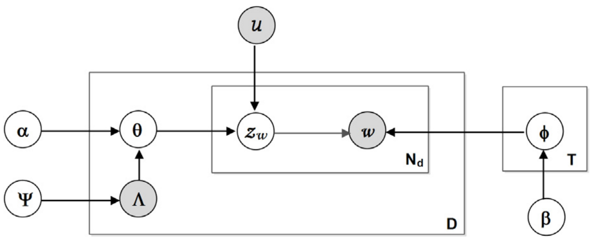


Fig. 2. The graphical model for the user-topic model based on LLDA.

We assume that there is a dictionary V containing all vocabulary appearing in user-generated texts (known as documents), and T predefined topics hiding in those documents. D is the collection of documents for all users, where the number of documents $|D|$ is equal to the number of users as one document strictly corresponds to one user after text integration. Each document $d \in D$ is represented by a word vector $\boldsymbol{w}^{(d)} = \{w_1, w_2, \dots, w_{N_d}\}$, where each $w_i \in V$ and N_d is the number of words in document d. A vector $\boldsymbol{\Lambda}^{(d)} = \{l_1, l_2, \dots, l_T\}$ ($l_i \in \{0, 1\}$) indicates the presence (as value 1) or absence (as value 0) of each topic in d.

From Fig. 2, we observe that the topics of document d for user u are drawn from a multinomial distribution $\boldsymbol{\theta}^{(d)} = \{\theta_1, \theta_2, \dots, \theta_T\}$ over T topics from a Dirichlet distribution with a parameter set $\boldsymbol{\alpha}$, which is restricted by a Bernoulli distribution $\boldsymbol{\Lambda}$ with a labeling prior probability $\boldsymbol{\Psi}$ to strictly ensure that each topic assignment z_w of word w in document d is only limited to the labels observed beforehand. Each topic distribution $\phi_t \in \boldsymbol{\phi}$ over words is associated with a multinomial distribution from a Dirichlet prior $\boldsymbol{\beta}$. While the distribution $\boldsymbol{\phi}$ just depends on $\boldsymbol{\beta}$, the distribution $\boldsymbol{\theta}$ depends on both $\boldsymbol{\alpha}$ and $\boldsymbol{\Lambda}$ represented by directed edges from $\boldsymbol{\alpha}$ and $\boldsymbol{\Lambda}$ to $\boldsymbol{\theta}$ in the plate in Fig. 2.

3.2.2. Model inference

The user-topic model is built on three sets of parameters, i.e., the user topic distributions $\boldsymbol{\theta}$, the topic occurrence distributions $\boldsymbol{\Lambda}$ in documents, and the T topic distributions $\boldsymbol{\phi}$. After the labels $\boldsymbol{\Lambda}$ are observed, the rest of the model is conditional independent from the labeling prior $\boldsymbol{\Psi}$ given $\boldsymbol{\Lambda}$, and these parameters can be estimated using Gibbs sampling as is the case in the traditional LDA [43]. Then, for each position in a document d, its sampling probability for a topic is given by:

$$P(z_i = j|\boldsymbol{z}_{-i}) \propto \frac{n^{w_i}_{-i,j} + \beta^{w_i}_j}{\sum_{w' \in V} n^{w'}_{-i,j} + \sum_{w' \in V} \beta^{w'}_j} \times \frac{n^{(d)}_{-i,j} + \alpha_j}{\sum_{j' \in T} n^{(d)}_{-i,j'} + \sum_{j' \in T} \alpha_{j'}} \tag{1}$$

where $z_i = j$ represents that the topic assignment of the ith word in the user document d is under topic j. Besides, $n^{w_i}_{-i,j}$ and $n^{(d)}_{-i,j}$ are the count of word w_i in topic j and the count of document d in topic j respectively, not including the current assignment z_i. $\beta^{w_i}_j$

[2] https://nlp.stanford.edu/software/tmt/tmt-0.4/

denotes the probability of word w_i belonging to topic j under the Dirichlet distribution with a prior β_j. All the parameters $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ in Eq. (1) are used to prevent the zero case in the counting process that some kinds of assignments may not occur due to the insufficient size of training data [38]. Then, given the document d, the probability of a user u_k with interests in topic j is computed as in Eq. (2).

$$P(t_{u_k} = j|d) \propto \prod_{i=1}^{N_d} P(z_i = j|\boldsymbol{z}_{-i}) \tag{2}$$

After the parameters are estimated, we can obtain two matrices, one of which is a $|V| \times T$ topic matrix over words, and the other is a $|D| \times T$ topic matrix over user documents. From the two matrices, the topic distribution over words ϕ and the topic distribution over users θ can be easily estimated by Eqs. (3) and (4), respectively.

$$\phi_{w_{i,j}} = \frac{n_{-i,j}^{w_i} + \beta_j^{w_i}}{\sum_{w' \in V}(n_{-i,j}^{w'} + \beta_j^{w'})} \tag{3}$$

$$\theta_{u_{k,j}} = \frac{n_{-i,j}^{(d)} + \alpha_j}{\sum_{j' \in T}(n_{-i,j'}^{(d)} + \alpha_{j'})} \tag{4}$$

Here, $\phi_{w_{i,j}}$ is the probability of word w_i used in topic j, and $\theta_{u_{k,j}}$ is the topic proportion of topic j in user u_k's document, where $\sum_{w_i \in V} \phi_{w_{i,j}} = 1$ and $\sum_{j \in T} \theta_{u_{k,j}} = 1$.

4. Topic-sensitive trust propagation approaches

In this section, we present the details of how to use the topic-sensitive approach to extend the topic-insensitive trust propagation methods and make them aware of different topics. Ziegler and Lausen [6] divided trust evaluation methods into two types: those using global trust metrics and those using local trust metrics. A global trust method is to offer a universal approved list or rank of trustees for all users, which means only one set of trustees and corresponding trust values will be released to the public without distinction. In contrast, a local trust method analyzes problems from the perspective of individuals by taking personal bias into account, and its results are disparate for different users. The proposed topic-sensitive approach can work on both global and local methods. In order to explain this better, we choose a global trust method (i.e., TrustRank [16]) and a local trust method (i.e., Appleseed [6]) as study cases to demonstrate the usage of our approach. Then, we summarize the main steps for extending most of the traditional trust propagation methods to be sensitive toward various topics in general.

4.1. TrustRank and Appleseed for trust evaluation

4.1.1. TrustRank

TrustRank, firstly proposed by Gyöngyi et al. [16], is a biased version of the PageRank algorithm [29], which selects a certain number of good users from the network as seeds, and then propagates trust from those seeds to the entire network and obtains the trust scores for all involved users. It is an iterative method that makes good nodes receive higher trust values, while bad nodes receive lower values after convergence. Although human experts are required to help manually identify the quality (i.e., good or bad) of those seeds, the number of seeds used in TrustRank is relatively small, and the improvement of performance is considerable [16,34]. As TrustRank cannot generate personalized trust scores for different people, it is a global trust evaluation method. The formula of trust evaluation in TrustRank is as follows:

$$tr(j) = \lambda \cdot \sum_{e_{ij} \in E} M_{ji} \cdot tr(i) + (1-\lambda) \cdot d_j \tag{5}$$

where $tr(j)$ is the trust score of node j, and M_{ji} is the corresponding element in the column-normalized transition matrix. e_{ij} is a directed edge from node i to node j, and E is the set of all edges. Let $e_{ij} \in E$ represent that edge e_{ij} exists in the set E, which actually is a condition used to find out all the ancestor nodes of node j. Trust in node i can propagate to node j, if and only if there is a directed edge pointing from node i to node j. Here, $\lambda \in [0, 1]$ is a decay factor for TrustRank as the proportion of trust distributed by one node to another will diminish when the distance between them increases. d_j is a flag that indicates whether node j is good or bad. If we define the set of good seeds as $\mathcal{S}^+$, then the value of d_i for node s_i is computed as follows:

$$d_i = \begin{cases} \frac{1}{|\mathcal{S}^+|} & \text{if} \quad s_i \in \mathcal{S}^+ \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

where $|\mathcal{S}^+|$ is the number of nodes in $\mathcal{S}^+$. Gyöngyi et al. proposed two strategies for selecting seeds: inverse PageRank and high PageRank [16]. The former method builds the seed set based on the number of outlinks, which means those selected seeds can maximize the coverage rate of the connected structure by propagating trust to as many nodes as possible. The latter method selects the seeds from those nodes with higher PageRank values since they might be more important than others [29]. The inverse PageRank strategy tries to enlarge the scale of reachable nodes by choosing the seeds with a high ability to distribute trust, while the high PageRank strategy emphasizes on identifying the trustworthiness of seeds with high influence as they are more likely to link to other trustworthy nodes.

4.1.2. Appleseed

Appleseed is a local trust propagation method inspired by spreading activation models in psychology, aiming to determine the rank of users in the network accurately. Ziegler and Lausen [6] introduced the concept of trust into the original model, and adopted energy transmission to simulate trust propagation. Different from global trust methods, Appleseed would choose a person as a seed to inject a certain amount of energy, which then flows into the network and is distributed to those reachable nodes. After convergence, the energy conserved in a node is regarded as the trust score it receives.

Compared with the original model, Appleseed is tailored in two facets to meet the demand of trust scenarios. First, it introduces a spreading factor $\lambda \in [0, 1]$ to control the proportion of energy flowing into the descendant nodes as trust decays when the spreading distance increases. Second, the edges of backward propagation are added into the network by simply creating a directed edge with weight $w = 1$ for each node from itself to the seed. By normalizing the weights of edges pointed from the same nodes, backward propagation can effectively avoid a poorly rated node getting a high trust score when the outdegree of its ancestors is low. It also eliminates the zero-outlink nodes as each node has at least one outlink [6,10]. The value of incoming trust for a node j is formulated as follows:

$$in(j) = \lambda \cdot \sum_{e_{ij} \in E} (in(i) \cdot \frac{W_{ij}}{\sum_{e_{ij'} \in E} W_{ij'}}) \tag{7}$$

where $in(j)$ represents the amount of trust flowing into node j from it ancestors, E is the set of directed edges in the graph, and e_{ij} is a directed edge pointing from node i to node j with weight W_{ij}. Trust in node i can flow into node j, if and only if there is a directed edge from node i to node j. So, the condition $e_{ij} \in E$ is used to find out all the ancestor nodes of node j. Then the trust score of node j is iteratively computed as follows:

$$tr(j)' = tr(j) + (1-\lambda) \cdot in(j)' \tag{8}$$

Please cite this article as: X. Chen, Y. Yuan, M.A. Orgun et al., A topic-sensitive trust evaluation approach for users in online communities, Knowledge-Based Systems (2020) 105546, https://doi.org/10.1016/j.knosys.2020.105546.

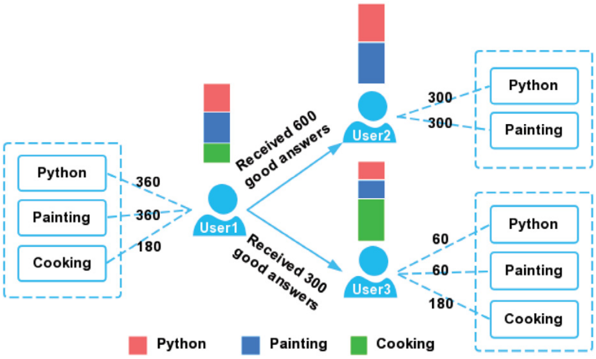


Fig. 3. An example of trust evaluation in a Q&A scenario with three topics.

where $tr(j)'$ is the new trust score of node j, which is equal to the sum of j's trust score in the previous iteration and the amount of energy kept in node j in the current iteration. In essence, the spreading factor λ is a trade-off between the ability to keep trust in a node itself and the ability to recommend other trustworthy nodes. With a low value of λ, Appleseed tends to give better ratings to those nodes that are close to the seed, while with a high value of λ, Appleseed allows trust to propagate further and wider in the network.

4.2. Topic coverage functions

Both TrustRank and Appleseed are graph-based methods, so a normalized transition matrix can be employed to represent the connectivity of nodes [6,16]. The elements in this matrix are the normalized weights of edges in the graph, which are usually obtained by counting the number of links between two nodes before normalization. However, these weights cannot reflect the topic relevance among users, which reduces the accuracy of trust evaluation when the application scenarios include multiple topics. In Fig. 3, we present a simple example of trust evaluation in a question-and-answer (Q&A) community to show the limitation of those methods without a strategy to distinguish the topics for different scenarios. Here, $user1$ has asked 900 questions about three different topics (i.e., Python, Painting, and Cooking), and has received 600 and 300 high-quality answers from $user2$ and $user3$, respectively. The weight of the edge from $user1$ to $user2$ is 0.67, which is double of that of $user1$ to $user3$. As a result, for those topic-insensitive methods, $user2$ will receive a higher overall trust rating than $user3$ without any distinction of these three topics. However, it is clear from the figure that $user2$ does not know anything about cooking, which means he is not reliable in this topic. Although $user3$ only answered 300 questions, he has 180 answers about cooking, which accounts for 60% of all his answers. In the scenario of seeking advice about cooking, we can say that $user3$ is more trustworthy than $user2$. Therefore, topic identification is quite significant for trust evaluation, especially for those scenarios covering many knowledge domains.

To solve this problem, we use a topic coverage matrix to compensate for the weakness of topic-free methods. In order to build the topic coverage matrix, we need to define the topic vectors first. In Fig. 3, the three colors represent the topic distribution for each user. A topic vector for a user indicates the level of expertise he has in different topics, which can be considered as the distribution over topics of that user. Fortunately, the method to obtain this distribution has been realized, that is the user topic distribution $\boldsymbol{\theta}$ in LLDA, which we have introduced in Section 3. Then, the topic vector of user u_i over T topics is denoted as $\boldsymbol{\theta}_{u_i} = \{\theta_{u_{i,1}}, \theta_{u_{i,2}}, \dots, \theta_{u_{i,T}}\}$. For a trust graph with N users, we can obtain a $N \times T$ user topic distribution matrix $\boldsymbol{\Theta}$ by aggregating all user topic vectors together, where $\sum_{i=1}^{N} \Theta_{ij} = 1$ for each topic $j \in T$ by normalizing each column.

The function of the topic coverage matrix is to estimate whether the topic proportion of user u_j can meet the demand of user u_i under topic t when there is a link from u_i to u_j. In order to figure it out, we define a topic coverage function, that is for a topic t, where there is a directed edge pointed from u_i to u_j, the coverage rate $\gamma_{ij}^{(t)}$ of the two users is computed as follows:

$$\gamma_{ij}^{(t)} = \begin{cases} (\frac{\Theta_{jt}}{\Theta_{it}})^q & \text{if} \quad \Theta_{jt} < \Theta_{it} \\ 1 & \text{otherwise} \end{cases} \tag{9}$$

where q is a positive value and Θ_{jt} is u_j's topic proportion of topic t in the distribution matrix $\boldsymbol{\Theta}$. Fig. 4 displays some topic coverage functions with different q when $x \in [0, 1]$. We divide the functions into two groups based on the value of q, where $q > 1$ in subfigure (a), and $0 < q < 1$ in subfigure (b). Let the function with $q = 1$ (the gray lines in subfigures) be the baseline for other functions. It is observed that all the curves are under the baseline in subfigure (a), but those curves are reversed in subfigure (b). Besides, the growth speed of curves in the two subfigures is different. When x approaches to 1, the curves rise more rapidly in subfigure (a), while in subfigure (b), the growth rate becomes slower. The coverage function is an asymmetric measure as $\gamma_{ij}^{(t)} \neq \gamma_{ji}^{(t)}$.

A topic coverage matrix for topic t is defined as $\boldsymbol{\Gamma}^{(t)} = [\gamma_{ij}^{(t)}]_{|N|\times|N|}$ that consists of the coverage rate between any two users over topic t. The number of topic coverage matrices is equal to the number of topics involved in the application scenarios. Since it is not clear how the topic coverage rate will develop and how it will influence trust ranking during propagation, we design the above two groups of functions to imitate two possible growth patterns. The effects of these proposed functions are tested in the experiments, and an optimal value of q would be selected for different trust evaluation methods.

4.3. Topic-sensitive TrustRank

In this section, we extend TrustRank to make it sensitive toward topics for trust evaluation. In order to implement the topic-sensitive TrustRank (TS-TrustRank), two main changes are required to the original method. First, the transition matrix $\boldsymbol{M}$ should be capable of recognizing the difference of topics since the matrix used in TrustRank does not consider the topic relevance between the two connected nodes. Second, the flag vector $\boldsymbol{d}$, which indicates the quality of users without distinguishing topics, should be updated to reveal the reliability of nodes for each topic separately.

Let $\boldsymbol{M}^{*(t)}$ represent the new transition matrix under topic t, and then each element $M_{ij}^{*(t)}$ in this matrix can be defined as follows:

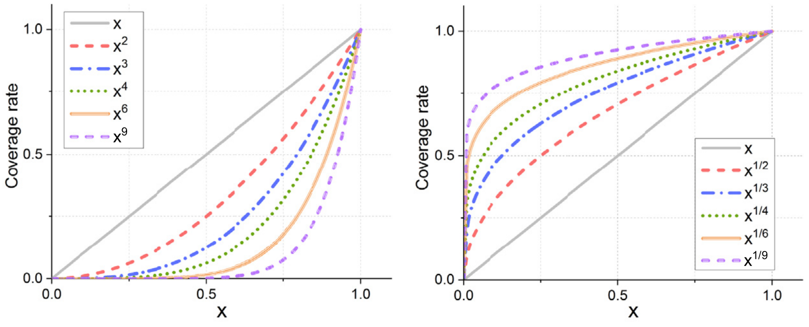
$$M_{ij}^{*(t)} = M_{ij} \cdot \gamma_{ij}^{(t)} \tag{10}$$

This matrix will be normalized to ensure that the sum of elements in each row i satisfies $\sum_{j=1}^{N} M_{ij}^{*(t)} = 1$. The flag vector for each topic is defined as follows:

$$d_i^{(t)} = \begin{cases} \frac{1}{|\mathcal{S}^{+(t)}|} & \text{if} \quad s_i \in \mathcal{S}^{+(t)} \\ 0 & \text{otherwise} \end{cases} \tag{11}$$

where $|S^{+(t)}|$ is the number of nodes in $S^{+(t)}$ which contains all the good seeds for topic t. For a trust scenario with T predefined topics, there are T topic-related transition matrices and T flag vectors to uncover the trustworthiness of users in different topics.

Please cite this article as: X. Chen, Y. Yuan, M.A. Orgun et al., A topic-sensitive trust evaluation approach for users in online communities, Knowledge-Based Systems (2020) 105546, https://doi.org/10.1016/j.knosys.2020.105546.



(a) $q > 1$ (b) $0 < q < 1$

Fig. 4. Topic coverage functions with different values of q. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Then Eq. (5) is reformulated as:

$$tr(j)^{(t)} = \lambda \cdot \sum_{e_{ij}\in E} M_{ji}^{*(t)} \cdot tr(i)^{(t)} + (1-\lambda) \cdot d_j^{*(t)} \tag{12}$$

where $d_j^{*(t)}$ is computed as:

$$d_j^{*(t)} = \frac{d_j^{(t)} \cdot \theta_{jt}}{\sum_{j'\in U} d_{j'}^{(t)} \cdot \theta_{j't}} \tag{13}$$

Here, $tr(j)^{(t)}$ is the trust score of node j on topic t, and $d_j^{*(t)}$ is a normalized factor combining the flag of node j and its topic relevance on topic t. The pseudocode of TS-TrustRank is shown in Algorithm 1. The lines from 3 to 16 display the details of how to compute the topic transition matrix $\boldsymbol{M}^{(t)}$ and the new flag vector $\boldsymbol{d}^{(t)}$ under topic t, and the lines from 17 to 23 show the process of iterative trust propagation in TS-TrustRank. The trust score of a user on topic t consists of two parts, one of which is the sum of the amount of trust received from people who know him on topic t, and the other one is the amount of trust received from a random person who does not necessarily know him. The algorithm does not stop until the sum of the increment of all trust scores under topic t between two iterations is no more than the predefined threshold. After the convergence of the algorithm, an array of trust scores for all users under topic t is returned.

4.4. Topic-sensitive Appleseed

Compared with the modification made on TrustRank, the procedure of improving Appleseed to make it aware of topics is relatively simple. Topic-sensitive Appleseed (TS-Appleseed) is implemented by readjusting the weight on each edge using the topic coverage matrix, which will then change the amount of energy flowing into each node. Therefore, Eq. (7) can be rewritten as follows:

$$in(j)^{(t)} = \lambda \cdot \sum_{e_{ij}\in E} (in(i)^{(t)} \cdot \frac{W_{ij}}{\sum_{e_{ij'}\in E} W_{ij'}} \cdot \gamma_{ij}^{(t)}) \tag{14}$$

where $in(j)^{(t)}$ is the amount of energy flowing into node j from its ancestors for topic t, and $\gamma_{ij}^{(t)}$ is the corresponding topic coverage rate in matrix $\Gamma^{(t)}$, which determines the topic relevance between the two nodes under topic t when trust is propagated from node i to node j. After the modification, Eq. (8) can still be applied to TS-Appleseed for trust score calculation. The complete pseudocode of the trust propagation process in TS-Appleseed is shown in Algorithm 2, where the lines from 5 to 22 display the details of the iterative trust propagation process. The trust score of a user on topic t consists of two parts, one of which is the trust score under topic t calculated in the previous iteration, and the other one is the amount of trust received from others and conserved in himself on that topic, which is not distributed to his acquaintances. When the sum of the increment of trust flowing into each node is no greater than the predefined threshold, the algorithm converges, and an array of trust scores for reachable users of that seed under topic t is returned.

Algorithm 1: Iterative Trust Propagation in TS-TrustRank

```
Input: G, trust graph $G = (U, E)$
       $\boldsymbol{M}$, transition matrix
       $l$, number of seeds
       $\lambda$, decay factor
       $\boldsymbol{\Gamma}^{(t)}$, topic coverage matrix under topic $t$
       $\boldsymbol{\Theta}_t$, $t$th column vector in the user topic distribution matrix
       $th$, convergence threshold
Output: $trust_k^{(t)}$, an array that stores the trust values of nodes under topic $t$ after the $k$th iteration.
1  $\boldsymbol{d}^{(t)} = \boldsymbol{0}_N$;
2  $k = 0$;
3  for each element $M_{ij} \in \boldsymbol{M}$ do
4      $M_{ij}^{*(t)} = M_{ij} \cdot \gamma_{ij}^{(t)}$
5  end
6  select $l$ seeds into $S$ according to an optional strategy;
7  $\boldsymbol{\sigma}$ = index positions of seeds in $U$;
8  $\boldsymbol{O}^{(t)}$ = quality of each seed (good or bad) in $S$ under topic $t$;
9  for each seed $s \in S$ do
10     if $O(\sigma(s))^{(t)}$ is good then
11         $d_{\sigma(s)}^{(t)} = 1$;
12     end
13 end
14 for each element $d_j^{(t)} \in \boldsymbol{d}^{(t)}$ do
15     $d_j^{*(t)} = \frac{d_j^{(t)} \cdot \theta_{jt}}{\sum_{j'\in U} d_{j'}^{(t)} \cdot \theta_{j't}}$
16 end
17 repeat
18     $k++$;
19     for each node $x \in U$ do
20         $trust_k(x)^{(t)} =$
           $\lambda \cdot \sum_{edge(u,x)\in E} M_{xu}^{*(t)} \cdot trust_{k-1}(u)^{(t)} + (1-\lambda) \cdot d_x^{*(t)}$;
21     end
22     $increment = \sum_{x\in U}(trust_k(x)^{(t)} - trust_{k-1}(x)^{(t)})$;
23 until $increment \leq th$;
24 return $trust_k^{(t)}$;
```

Please cite this article as: X. Chen, Y. Yuan, M.A. Orgun et al., A topic-sensitive trust evaluation approach for users in online communities, Knowledge-Based Systems (2020) 105546, https://doi.org/10.1016/j.knosys.2020.105546.

4.5. Main procedures for implementing topic-sensitive trust evaluation methods

Usually, there are four main steps for extending topic-free trust propagation methods using the topic-sensitive analysis approach. First, topic distributions θ over users are computed by implementing the user-topic model, which will be used in the third step. Second, all the topic-involved components in the original algorithms are required to be identified. For most of the trust propagation methods, there is only one component that relates to the topic data, that is the transition matrix. However, when other factors exist for correlating the estimated results, we need to find them out as well, such as the flag d in TrustRank. Third, the user topic distributions are utilized to construct the topic coverage matrices for all the involved topics, and the optimal value of q is estimated by several tests and experiments. Finally, the topic coverage matrices and user topic distributions are integrated into the identified components in the original algorithms, which extend those topic-free trust propagation methods to be sensitive toward different topics.

5. Experimental results

In Section 4, we present the implementation of two topic-sensitive trust evaluation methods based on two classic topic-insensitive trust propagation approaches. These methods estimate the trust rankings and trust values of involved users by taking into consideration both the topic interests of individuals and the topic relevance between them. In this section, in order to evaluate the performance of the proposed methods, we conduct experiments over a real-world dataset obtained from Stack Exchange and present a detailed analysis of the results.

5.1. Dataset

Stack Exchange [44] is an online Q&A website that allows users to ask and answer questions in 174 different topics. On Stack Exchange, a reliable user gains more reputation because of his contribution to the positive development of the Q&A community, who usually has professional knowledge in at least one domain and behaves in a good manner on the website [44]. We select this dataset to conduct experiments for two reasons. Firstly, Stack Exchange provides categories of topics in its directory, which is an outstanding resource of training labels for LLDA. Secondly, Stack Exchange focuses on the acquisition of domain-specific knowledge rather than a subjective discussion between questioners and answers, so there is no function for users to follow someone or be followed by others, which makes them pay more attention to the quality of users' posts. In other words, participants tend to express their trust opinions toward others according to the real level of expertise users have in specific areas other than the social relationships or social intimacy between them. Therefore, we conduct our experiments on the Stack Exchange dataset released by its official team on Internet Archive.[3]

The original Stack Exchange dataset is quite large, which contains 174 different topics and millions of records. In order to reduce the complexity and improve the feasibility of the experiments, we select data of three categories from the dataset to conduct the experiments. The three categories are *Electronical Engineering*,[4] *Physics*,[5] and *Cross Validated*,[6] where present Q&A regarding electronics and electrical engineering, physics, statistics and data analysis, respectively. There are three reasons for selecting these three topics. First, the selected three categories possess a large number of questions and answers, which provide a prominent corpus for topic analysis in the user-topic model. Second, these categories are relatively independent. Some of the categories on Stack Exchange are not incompatible, which makes it difficult for users to identify the boundary of domain knowledge when they offer ratings to those posts. This ambiguity makes the ratings inaccurate and influences the comparison results. The incompatibility can effectively ensure that the user ratings of each topic solely depend on the contributions of the corresponding topic without the influence of others. In addition, the distinction of some overlapping categories is vague, which results in complicated discussions for the importance of identifying trust on those similar categories. For example, the posts under the category of *Ask Ubuntu* are Q&A about Ubuntu, and those under *Unix & Linux* are Q&A for Linux systems. Some overlaps exist in these two categories as Ubuntu belongs to the family of Linux systems, but they are not completely the same as other systems also exist in the Linux family. These overlaps are not easy to be defined and quantified. It is also difficult to reach a consensus about the boundary and significance of identifying the trustworthiness of users on these similar categories. Generally, when overlaps exist between different categories, we consider that they can be divided into some smaller independent topics. Third, although the topics of these three categories are completely independent, there is still a considerable size of users involved

Algorithm 2: Iterative Trust Propagation in TS-Appleseed

```
Input: $G$, trust graph $G = (U, E)$
       $s$, seed for energy injection where $s \in U$
       $e$, energy flows into $s$
       $\lambda$, spreading factor
       $\boldsymbol{\Gamma}^{(t)}$, topic coverage matrix under topic $t$
       $th$, convergence threshold
Output: $trust_k^{(t)}$, an array that stores the trust values of
        nodes under topic $t$ after the $k$th iteration
$in_0(s)^{(t)} = e$;
$trust_0(s)^{(t)} = 0$;
$k = 0$;
$U_0 = \{s\}$;
repeat
    $k++$;
    $U_k = U_{k-1}$;
    set $in_k(x)^{(t)} = 0$ for node $x \in U_{k-1}$;
    for each node $x \in U_{k-1}$ do
        $trust_k(x)^{(t)} = trust_{k-1}(x)^{(t)} + (1 - \lambda) \cdot in_{k-1}(x)^{(t)}$;
        for each edge$(x, u) \in E$ do
            if node $u \notin U_k$ then
                add node $u$ into $U_k$;
                set $trust_k(u)^{(t)} = 0$ and $in_k(u)^{(t)}$=0;
                add $edge(u, s)$ and set its weight $w(u, s) = 1$;
            end
            $\bar{w} = w(x, u)/\sum_{edge(x,u')\in E} w(x, u')$;
            $in_k(u)^{(t)} = in_k(u)^{(t)} + \lambda \cdot in_{k-1}(x)^{(t)} \cdot \bar{w} \cdot \gamma_{xu}^{(t)}$;
        end
    end
    $increment = \sum_{x\in U_k}(trust_k(x)^{(t)} - trust_{k-1}(x)^{(t)})$;
until $increment \leq th$;
return $trust_k^{(t)}$ for nodes in $U_k$;
```

[3] https://archive.org/details/stackexchange

[4] https://electronics.stackexchange.com

[5] https://physics.stackexchange.com

[6] https://stats.stackexchange.com

Table 1
Subset of Stack Exchange dataset used in experiments.

Category	#Users	#Questions	#Answers	Abbreviation
Electronical engineering	670	37,768	47,403	Elec
Physics	670	36,376	43,983	Phy
Cross validated	670	28,631	33,852	Stats

* *# represents the number of items.*

Table 2
The correlation matrix of user reputation rankings on the three topics based on Spearman's coefficient ρ.

Spearman's ρ		Topic		
		Elec	Phy	Stats
Topic	Elec	1.000	−0.231	−0.358
	Phy	−0.231	1.000	−0.260
	Stats	−0.358	−0.260	1.000

* *2-tailed significance tests show that all the p-values are smaller than 0.01.*

in them simultaneously, which makes it an excellent dataset for topic-related trust evaluation.

Although there are a large number of users involved in each category, most of them are inactive as they do not have enough interactions with others. Texts (including questions and answers) generated by them are insufficient for topic analysis, so we refine the data to generate a subset by removing those users whose number of posted questions and answers is no more than 20 in each category. After the filtering, only 670 users are left in the subset, and the associated questions and answers used for topic analysis in experiments are those generated by these users. The details of the dataset are shown in Table 1. By ranking the users across topics according to their reputation, we find that topic recognition is necessary before evaluating trust. The correlation matrix of user reputation rankings under the three topics is shown in Table 2. Here, we use Spearman's coefficient ρ which will be introduced in Section 5.3 in detail. Significance tests show that these results are statistically significant as all the p-values are much smaller than 0.01. It can be observed that the values of ρ are quite low for any two topics indicating that their reputation rankings are strongly different. If trust of a person is invariable across topics, the values of rank correlation for different topics shall be close to 1. By checking the complete dataset, we observe that almost no one has the same rankings across the three topics, which indicates that the difference of topics should not be ignored when evaluating trust.

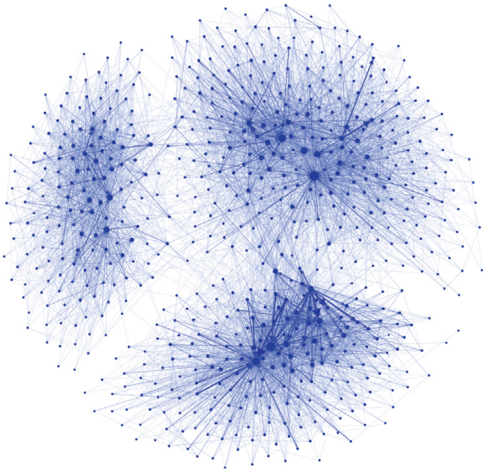


Fig. 5. The trust graph of 670 users based on their Q&A relationships.

Table 3
The accuracy metrics.

Metrics	Computing equation
Precision	$\frac{\lvert\{u \in U \mid tr(u) \geq \delta \text{ and } re(u) \geq \delta\}\rvert}{\lvert\{u \in U \mid tr(u) \geq \delta\}\rvert}$
Recall	$\frac{\lvert\{u \in U \mid tr(u) \geq \delta \text{ and } re(u) \geq \delta\}\rvert}{\lvert\{u \in U \mid re(u) \geq \delta\}\rvert}$
True positive rate	$\frac{\lvert\{u \in U \mid tr(u) \geq \delta \text{ and } re(u) \geq \delta\}\rvert}{\lvert\{u \in U \mid re(u) \geq \delta\}\rvert}$
False positive rate	$\frac{\lvert\{u \in U \mid tr(u) \geq \delta \text{ and } re(u) < \delta\}\rvert}{\lvert\{u \in U \mid re(u) < \delta\}\rvert}$

* *tr(u) represents the trust scores generated by the algorithms, and re(u) represents the sum of scores of involved posts for users given by Stack Exchange.*
** *U is the set of all users involved in the experiments, and |U| is the number of users in U.*

5.2. Trust graph construction

The proposed approach attempts to predict trust for users under different topics using the same link structure without topic bias. Therefore, the network is constructed by combining all users' Q&A relationships on all the topics. Based on these relationships, we can build a directed graph $G = (U, E)$ to represent their link structure. Here, U is a set of nodes representing users, and E is a set of directed edges recording the Q&A relationships between any two users. A directed edge $e_{ij} = (u_i, u_j)$ indicates user u_j answers u_i's questions, where both u_i and u_j are nodes belonging to U. Then, we can obtain a square $|U| \times |U|$ adjacency matrix according to the graph G, where each element A_{ij} in the matrix represents the number of answers that u_j gives to u_i. Stack Exchange allows users to answer the questions asked by themselves, which will create an edge from a vertex to itself, known as loops [16,29]. We eliminate these loops from the graph as a person would always trust himself. The elimination makes the diagonal elements of the matrix all zeros. Fig. 5 illustrates the Q&A structure of 670 users, where the node size will be bigger for a user who answers more questions, and where an edge with larger A_{ij} will gain a darker color and a thicker line. Based on the adjacency matrix, the weight W_{ij} of each edge e_{ij}, also considered as trust weights u_j received from u_i, can be calculated as follows:

$$W_{ij} = \begin{cases} \frac{A_{ij}}{\sum_{j'=1}^{|U|} A_{ij'}} & \text{if } \sum_{j'=1}^{|U|} A_{ij'} \neq 0, \\ 0 & \text{otherwise} \end{cases} \tag{15}$$

It should be noted that W_{ij} is usually not equal to W_{ji}, and $\sum_{j'=1}^{|U|} W_{ij'} = 1$. Then, we can generate the transition matrix $\boldsymbol{M} = [M_{ij}]_{|U|\times|U|}$ to represent the transition probability from u_i to u_j, where $M_{ij} = W_{ij}$. There is no constraint on the matrix for Appleseed and TS-Appleseed so that the original transition matrix can be directly used. However, for TrustRank and TS-TrustRank, the transition matrix $\boldsymbol{M}$ must be stochastic [16], so the rows without non-zero elements are replaced by a vector with all elements equal to $1/|U|$.

5.3. Evaluation metrics

Stack Exchange has its algorithm to compute the reputation of users in different top-level categories by counting the high-quality questions and useful answers of users. Votes on these posts are the primary means to gain or lose reputation, where upvotes help improve reputation, while downvotes cause loss of reputation [44]. Each question or answer has a score, which generally is the number of upvotes on a post minus the number of downvotes. Since the trust graph we use in the experiments is a subgraph extracted from the entire network of Stack Exchange,

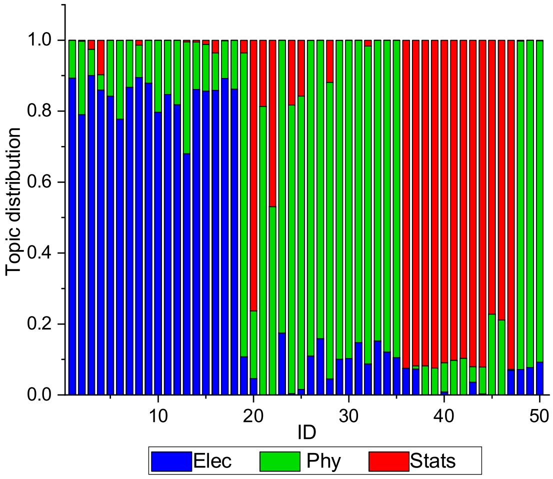


Fig. 6. Topic distributions of 50 randomly selected users.

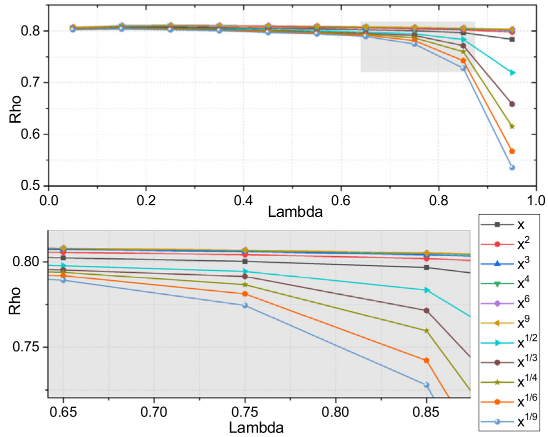


Fig. 7. Spearman's coefficient ρ of different topic coverage functions across λ for TS-TrustRank. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Table 4
Representative words in the three selected topics recognized by the user-topic model.

Topic	Top 10 representative words
Elec	Input, Resistor, Signal, Supply, Frequency, Device, Load, Pin, Capacitor, Battery
Phy	Force, Mass, Vector, Space, Equation, Theory, Quantum, State, Particle, Velocity
Stats	Distribution, Test, Mean, Sample, Regression, Value, Variable, Sum, Number, Probability

we use the sum of scores of users' posts in each topic as the ground truth of user trust scores. It is considered as a rough measurement of reputations for the incomplete graph to indicate how much the community can trust a user. In order to maintain the consistency of the value range, we set the scores given by Stack Exchange and the scores inferred by trust evaluation approaches in the same interval of values.

The evaluation of results is made from two aspects: the consistency of trust rankings and the accuracy of estimated trust values. To measure the consistency of trust rankings, we leverage Spearman's rank correlation coefficient ρ in the evaluation process, which can measure the similarity between any two rankings. For two variables $\boldsymbol{x}$ and $\boldsymbol{y}$, the full version of Spearman's formula to deal with the tied ranks [45] is as follows:

$$\rho = \frac{\sum_{i=1}^{N}(R(x_i) - R(\bar{x}))(R(y_i) - R(\bar{y}))}{\sqrt{\sum_{i=1}^{N}(R(x_i) - R(\bar{x}))^2 \cdot \sum_{i=1}^{N}(R(y_i) - R(\bar{y}))^2}} \tag{16}$$

where $R(x_i)$ and $R(y_i)$ are the corresponding rankings of value x_i and value y_i, $R(\bar{x})$ and $R(\bar{y})$ are the rankings of the mean values of $\boldsymbol{x}$ and $\boldsymbol{y}$. If the rankings of $\boldsymbol{x}$ and $\boldsymbol{y}$ are identical, the coefficient $\rho = 1$, while when they are fully opposed, the coefficient $\rho = -1$.

In order to evaluate the accuracy of estimated trust values, we formulate trust assessment as a binary decision problem. Then, we use Precision–Recall (PR) curves and Receiver Operator Characteristic (ROC) curves to show the performance of trust classification of the selected methods across different thresholds. PR and ROC curves are two useful measures used to evaluate the binary classification models [46]. Four metrics are involved in these two kinds of plots, namely, true positive rate (TPR), false positive rate (FPR), precision, and recall. The PR curve uses recall on the x-axis and precision on the y-axis, whereas the ROC curve uses FPR on the x-axis and TPR on the y-axis. These metrics are usually used in machine learning, but they can be applied in trust analysis as well with some modifications [23,47]. We define a trustworthy user as a person with a trust score or reputation of no less than value δ, denoted as $tr(u) \geq \delta$ or $re(u) \geq \delta$. Then all the involved metrics are defined as shown in Table 3. Here, $|\{u \in U|tr(u) \geq \delta\}|$ is the number of users asserted to be trustworthy by the trust evaluation approaches, whereas $|\{u \in U|re(u) \geq \delta\}|$ is that of the genuinely trustworthy people in practice. $|\{u \in U|tr(u) \geq \delta$ and $re(u) \geq \delta\}|$ represents the number of users who are correctly classified as trustworthy persons, while $|\{u \in U|tr(u) \geq \delta$ and $re(u) < \delta\}|$ denotes the number of users who are incorrectly classified as trusted people. PR curves show the trade-off between precision and recall across different thresholds, and ROC curves show the disparity between the correctly classified positive samples and incorrectly classified negative samples. A perfect PR curve shall be in the upper-right corner of the plot, whereas an ideal ROC curve would be close to the upper-left corner [46]. Usually, a visual inspection of curves is a common way to compare the performance of two approaches when the difference between their curves is distinguishable. When this difference is not easy to distinguish, the area under the curve (AUC) can be employed as a general measure to compare the performance of the selected algorithms, where a larger area under the curve represents a better performance of the algorithm. The experimental results of these metrics are presented in the next section.

5.4. Results

5.4.1. Topic distributions

As mentioned in Section 3, we use the user-topic model to automatically learn topics and topic distributions over users from the content of Q&A documents. In the experiments, we implement the user-topic model with 1000 iterations of Gibbs sampling [43] to generate the topic distributions of documents and users using Stanford Topic Modeling Toolbox (See footnote 2). Table 4 presents the top 10 representative words of the three topics. It can be observed that words recognized in the corresponding topics are fine-grained and meaningful. Fig. 6 illustrates the topic distributions over the three topics of 50 randomly selected users, which clearly shows that different users have different topic interests.

5.4.2. Comparison of topic coverage functions

In Section 4.2, we have presented some topic coverage functions with different values of q. Here, we conduct experiments

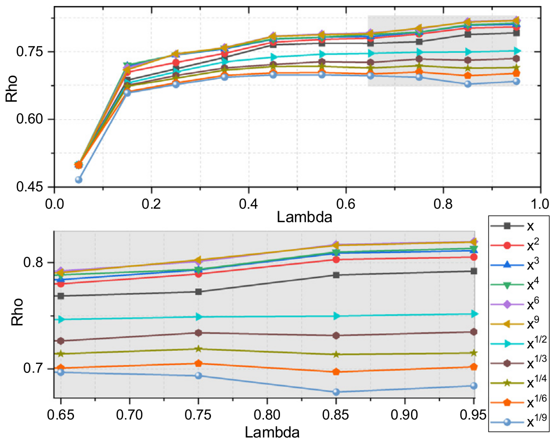


Fig. 8. Spearman's coefficient ρ of different topic coverage functions across λ for TS-Appleseed. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

with these functions on TS-TrustRank and TS-Appleseed and compare the results according to Spearman's coefficient ρ to disclose the effect of different q for different topic-sensitive methods. Figs. 7 and 8 show how coefficient ρ changes with topic coverage functions across decay factor (or spreading factor) λ for TS-TrustRank and TS-Appleseed, respectively. The gray subfigures in the bottom of both figures are the enlarged images of the corresponding gray zones in the top subfigures.

For TS-TrustRank, when λ is smaller than 0.65, rank correlation ρ hardly changes across different values q, while when λ is greater than 0.65, different topic coverage functions have a distinct influence on ρ. For those functions with $q < 1$, ρ changes with λ, where the smaller q is, the faster ρ drops across λ as λ approaches to 1. In Fig. 7, when $\lambda \geq 0.65$, the Spearman's coefficient ρ declines rapidly, especially when $q = 1/9$. For those functions with $q \geq 1$, there is no significant change on ρ along with λ, but their values of ρ are greater than those generated by functions with $q < 1$, particularly when λ is quite large.

For TS-Appleseed, the pattern of changes is different from that of TS-TrustRank. The value of ρ generated by some functions like $f = x^{1/9}$ drops at the point of $\lambda = 0.75$, but it does not change the overall trend, where in general, the Spearman's coefficient ρ increases as λ becomes larger for all the topic coverage functions. Moreover, the larger the value q is, the greater ρ will be.

5.4.3. *Accuracy of topic-sensitive methods*

In order to show the effect of the topic-sensitive approach, we conduct experiments and compare the performance of TrustRank and Appleseed in both topic-involved and topic-free versions under the three topics. We first investigate the influence of the parameter λ on coefficient ρ to the approaches across topics and then compare the accuracy metrics of various algorithms after finding the optimal parameters. It is worth noting that the used ground truths are topic-specific. Different topics have distinct ground truths as users' scores are calculated by adding all their received scores on the corresponding category separately. All the experiments utilize the same network without any topic bias, and the experiments conducted on the same category share the same ground truth.

Fig. 9 displays the way in which ρ changes with the parameter λ on the three topics and on average, when selecting the optimal topic coverage functions for TS-TrustRank and TS-Appleseed. By analyzing the results of different topic coverage functions, we choose $f(x) = x^9$ and $f(x) = x^6$ as the final functions used in TS-TrustRank and TS-Appleseed, respectively. The four subfigures show that TS-TrustRank and TrustRank are less sensitive to the parameter λ, especially for TS-TrustRank, which hardly changes across various λ. For TS-Appleseed and Appleseed, the curves of ρ rise fast first, and then change slightly or almost remain stable. The overall Spearman's coefficient ρ of topic-sensitive approaches is higher than the corresponding topic-insensitive methods. TrustRank always results in the lowest value of ρ as λ varies. Except for the subfigure (c) where Appleseed produces a better result of ρ than the TS-TrustRank for topic *Stats* when $\lambda \geq 0.15$, TS-TrustRank and TS-Appleseed usually obtain the first and second best results of Spearman's rank correlation. The performance of the extended topic-sensitive methods is always better than those of their corresponding original topic-free methods. In addition, the average performance of topic-sensitive approaches is generally better than those of original topic-insensitive approaches. Topic-sensitive methods are more stable than the traditional topic-free methods as the rank correlation generated by them is always relatively high over different topics, while the good performance of topic-insensitive methods seems to be a coincidence just for some kinds of data. Therefore, the proposed topic-sensitive framework has a significant improvement in the consistency of trust rankings across topics.

After observing the pattern of Spearman's coefficient changing with the parameter λ, we set the optimal parameter λ for the four methods, where $\lambda = 0.85$ for TS-TrustRank and TrustRank, while $\lambda = 0.95$ for TS-Appleseed and Appleseed. Then the specific values of metrics can be obtained. Table 5 displays the values of Spearman's coefficient ρ and its corresponding p-value. For the topics *Elec* and *Phy*, TS-TrustRank achieves the best results with $\rho = 0.825$ and $\rho = 0.850$, respectively, and TS-Appleseed yields the second best rank correlation coefficients with $\rho = 0.791$ and $\rho = 0.816$. However, for the topic *Stats*, TS-Appleseed yields the best result of ρ where $\rho = 0.852$.

We note that Appleseed gains the second highest coefficient on the topic *Stats* with $\rho = 0.839$, which is greater than that of TS-TrustRank with $\rho = 0.770$. It seems that the Appleseed series methods are more suitable for the data on the topic of *Stats*. To explain the reason for this phenomenon, we check the data on *Stats* and find that the percentage of users with quite low scores on that category is higher than those on *Elec* and *Phy*. Besides, the mean value of *Stats* is also lower than those of *Elec* and *Phy*. Appleseed series methods are local trust metrics without a strategy to handle the unreachable nodes of the source node (known as unreferenced nodes [16]), whereas TrustRank series approaches are global trust metrics capable of dealing with all involved nodes. Therefore, the predicted trust values of Appleseed

Table 5
Spearman's rank correlations of the four methods on the three topics.

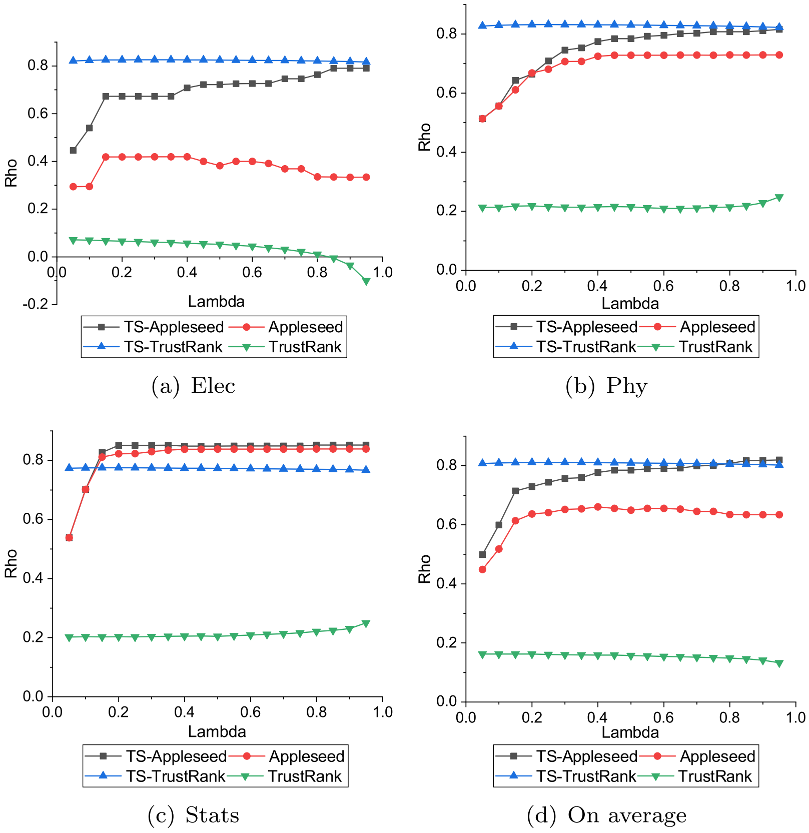
Method	Correlation	Topic		
		Elec	Phy	Stats
TS-TrustRank	Coefficient ρ p-value	**0.825** 2.08×10^{-167}	**0.850** 1.04×10^{-187}	0.770 1.26×10^{-132}
TrustRank	Coefficient ρ p-value	-0.005 8.95×10^{-1}	0.219 9.88×10^{-9}	0.224 4.31×10^{-9}
TS-Appleseed	Coefficient ρ p-value	0.791 1.79×10^{-144}	0.816 2.63×10^{-161}	**0.852** 3.45×10^{-190}
Appleseed	Coefficient ρ p-value	0.334 6.18×10^{-19}	0.730 2.64×10^{-112}	0.839 1.24×10^{-178}

* *The topic coverage function of TS-TrustRank is $f(x) = x^9$, while that of TS-Appleseed is $f(x) = x^6$.*

** *The decay factor of TS-TrustRank and TrustRank is $\lambda = 0.85$, while the spreading factor of TS-Appleseed and Appleseed is $\lambda = 0.95$.*

*** *The bold values indicate the best results for the three topics.*

Please cite this article as: X. Chen, Y. Yuan, M.A. Orgun et al., A topic-sensitive trust evaluation approach for users in online communities, Knowledge-Based Systems (2020) 105546, https://doi.org/10.1016/j.knosys.2020.105546.



(a) Elec

(b) Phy

(c) Stats

(d) On average

Fig. 9. Spearman's coefficient ρ with the ground truth across λ.

Table 6
AUC of the four methods on the three topics.

Method	AUC of PR curves			AUC of ROC curves		
	Elec	Phy	Stats	Elec	Phy	Stats
TS-TrustRank	**0.905**	**0.787**	**0.917**	**0.976**	**0.935**	**0.981**
TrustRank	0.298	0.416	0.294	0.723	0.782	0.735
TS-Appleseed	0.772	0.672	0.848	0.786	0.791	0.902
Appleseed	0.488	0.644	0.847	0.731	0.747	0.898

* *The bold values indicate the best results for the three topics.*

series methods for those unreachable nodes are lower than those of TrustRank series. Because more users' trust values on the topic *Stats* locate in the smaller value range, the discrepancies between the predicted values of Appleseed series and the ground truth are smaller. Then, the values of rank correlations for Appleseed series are higher than those for TrustRank series. Overall, TrustRank yields the worst results of ρ for all the three topics. The values of ρ are always high and not varying much for topic-sensitive methods, while those values are usually low and change greatly for topic-free methods. Except for the p-value of TrustRank under the topic *Elec*, other p-values for all the methods across the three topics are quite small (far less than 0.01), which means these results are typically considered statistically significant.

Fig. 10 shows the PR and ROC curves of the four methods on the three topics across different thresholds. The corresponding areas under these curves are presented in Table 6. We say that one curve dominates other curves when all those curves are beneath it or equal to it [46]. From Fig. 10, we observe that the curves of TS-TrustRank always dominate those of TrustRank in both PR and ROC spaces across all the three topics. On the other hand, the PR curves of TrustRank on all the three topics always stay at a low level, which indicates its performance is not good on the selected topics. The gaps between the curves of TS-TrustRank and TrustRank are significant in both PR and ROC spaces. As shown in Table 6, TS-TrustRank achieves better results of AUC for both curves on all the topics. Therefore, the performance of TS-TrusRank is superior to that of TrustRank. The curves of TS-Appleseed also dominate the curves of Appleseed in both PR and ROC spaces across the three topics. The advantages of TS-Appleseed over Appleseed can be intuitively observed from Fig. 10 for topics *Elec* and *Phy*, where a significant gap exists between the corresponding curves of these two methods. From Table 6, it can be observed that TS-Appleseed obtains higher values of AUC than those of Appleseed on all the three topics in varying degrees, which indicates that the performance of TS-Appleseed is better than that of its topic-free version. Therefore, the proposed topic-sensitive methods outperform those topic-insensitive approaches.

It is worth noting that the improvement of TS-TrustRank over TrustRank is significant and stable on all the topics, but that of TS-Appleseed over Appleseed varies for different topics. For *Stats*, the distances between the curves of TS-Appleseed and Appleseed are not distinct, and the gaps between their values of AUC are small in both PR and ROC spaces. We observe that there might be two possible reasons for this phenomenon. First, as we have mentioned before, the percentage of users with low scores on *Stats* is higher than those on *Elec* and *Phy*, and Appleseed series methods would not allocate trust to those unreferenced nodes. Due to the particular characteristics of the data, Appleseed achieves an outstanding result on *Stats*, and the topic-sensitive analysis cannot fully achieve its tuning effect. Second, Appleseed series methods are local trust propagation methods, which means they allow personal bias whereby individuals have different trust assertions toward the same person. The ground truths used in the experiments are generated by the community's algorithm, which abandon the personal bias and conflicting opinions to reach a consensus throughout the whole community. These official trust scores are the approximate values of the real personal trust assertions, which can show the overall trend of user trust with some potential discrepancies. These discrepancies might reduce the distance between the curves of TS-Appleseed and Appleseed to some extent. For Appleseed, the performance on topic *Stats* is better than that on topics *Elec* and *Phy*, which leaves a smaller space for TS-Appleseed to improve where a slight discrepancy would make more impact on the results of *Stats* than the other topics. Generally, TS-Appleseed obtains relatively high values in both the rank correlation and the accuracy metrics, which shows that its overall performance is positive for all the three topics. In particular, it gains a significant improvement over Appleseed in Spearman's coefficient ρ, which ensures that it can yield a highly ordered ranking.

5.5. Discussion

We can observe that the performance of TS-TrustRank is better than that of TS-Appleseed since the topic-related data are considered twice in TS-TrustRank including the topic-related transition matrix $\boldsymbol{M}^{*(t)}$ and the topic-aware flag vector $\boldsymbol{d}^{*(t)}$, while there is only one consideration of topic data in TS-Appleseed, i.e., the weight reassignment by adding $\boldsymbol{\gamma}^{(t)}$. Therefore, the adjustment effect of the topic-sensitive framework on TrustRank is more evident than that on Appleseed. In this paper, we do not intend to compare the performance of different types of trust propagation methods extensively, which greatly depends on the characteristics of the original methods and used data. Instead, we focus on the improvement of the methods from the same family, that is those topic-sensitive trust approaches versus their original topic-free versions. We can see from Tables 5 and 6 that topic-sensitive methods certainly show improvement over the topic-insensitive methods, although sometimes the degree of improvement varies on different topics.

Generally, the topic-sensitive approach can improve the performance of topic-insensitive trust evaluation, including global and local propagation methods in both the ranking consistency and the classification accuracy. From the distinction of performance for different types of trust evaluation methods, we note that the choices of the original methods are also important. In this paper, we select two typical trust methods to show the effect of our approach in a direct way. However, it is worth noting that a careful selection of the fundamental trust propagation methods according to the characteristics of the given data can maximize the effectiveness of topic-sensitive analysis.

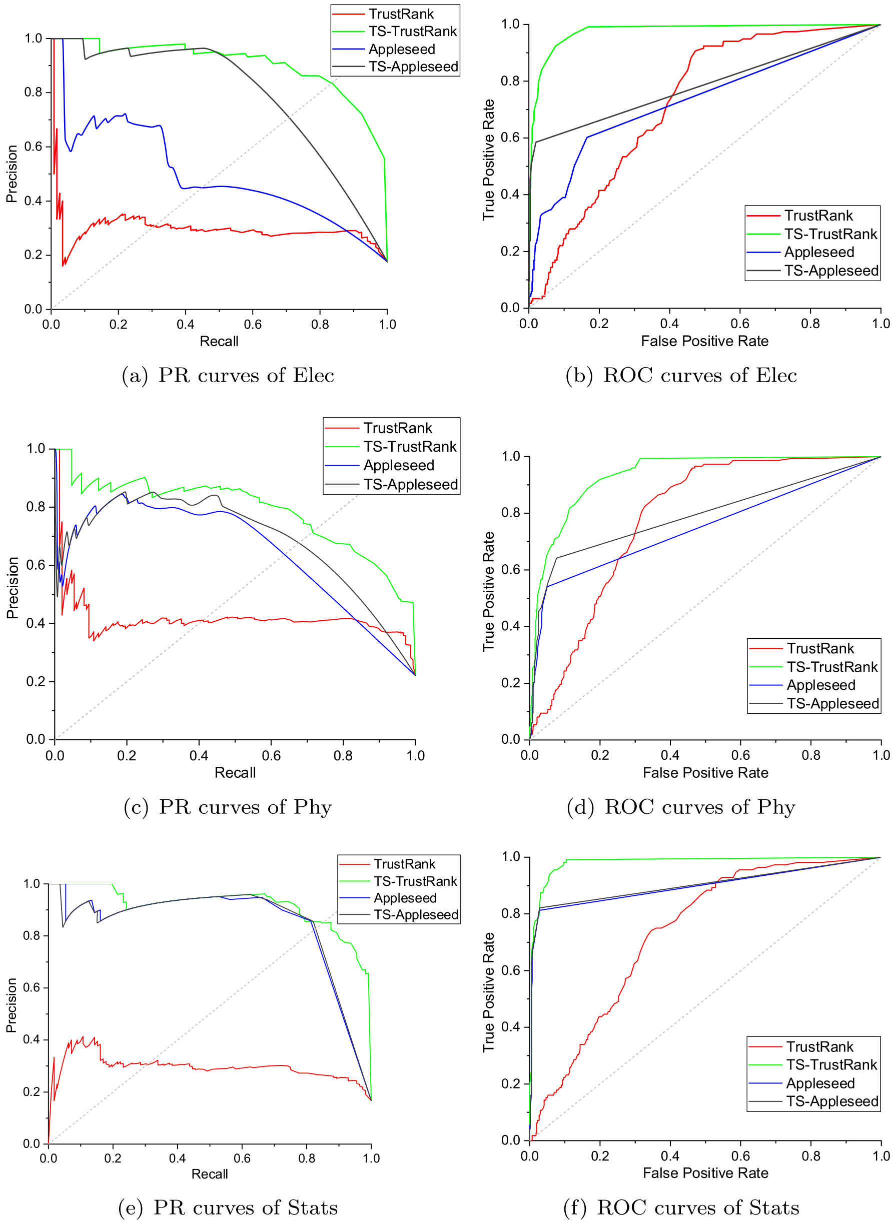
Except for the proposed topic-sensitive trust approaches, topic-specific trust models are another choice used to address the issue of context-aware trust. A topic-specific trust model runs a trust evaluation method by only utilizing the link and context data specific to the topic under analysis. To obtain the results of different topics, the topic-specific trust model would run multiple times. The topic-specific methods are applicable only when both the link data and the topic data are available. The procedures of topic-specific approaches are simpler than those of topic-sensitive methods when both types of data are explicitly provided. However, these data are usually not separately available as all the information of topics and structures is mixed and hidden in user data. In the experiments, we use the dataset from Stack Exchange which overtly provides both kinds of data for different categories. We mix the data from the selected categories together to simulate practical situations in most of the application scenarios and use the topic-sensitive approaches to extract the topic information from the mixtures. In order to implement the topic-sensitive evaluation methods, we need to distill the topic information from the raw data and use the same mixed link structure by introducing the topic coverage functions and matrices. However, for topic-specific approaches, we need to extract both the data of structures and topics for a specific topic. Therefore, when the data from different topics are mixed and cannot be easily recognized, the topic-sensitive approaches are more applicable. When the topic and link data can be easily obtained and separated, the topic-specific methods are more straightforward to implement. Generally, topic-sensitive trust approaches are more adaptive as they do not require the involved data to be fully divided according to the specific topics.

6. Conclusion and future work

In this paper, we have proposed a topic-sensitive approach that improves the performance of trust evaluation by recognizing different topics underlying trust, which is mostly neglected by the existing trust evaluation methods. First, we have built a topic-sensitive framework to systematically define the architecture of topic-sensitive trust analysis based on traditional trust evaluation methods. Second, a user-topic model has been proposed to automatically extract potential topics of individuals from user-generated content using LLDA. Then, we have designed a topic coverage function to discover the topic relevance between users by utilizing the derived topic data. In addition, the key procedures for extending topic-free trust methods are summarized. Two topic-insensitive trust propagation methods have been employed and extended to become sensitive toward different topics among various trust scenarios.

We have conducted experiments on a real-world dataset from Stack Exchange. The topic extraction result shows that the user-topic model can effectively identify meaningful and representative words in each topic and recognize the specific proportions of possible topics in documents for users. By comparing the results of Spearman's coefficient ρ for different topic coverage functions, we have found the optimal function for each topic-sensitive method. The comparison of four methods, including TS-TrustRank, TS-Appleseed, and their topic-free versions, has shown that the topic-sensitive approach improves the performance of trust evaluation in both the ranking consistency and the classification accuracy for all the three topics. We consider the topic-sensitive approach as an integral component in the trust evaluation system, which is widely applicable in many trust methods with appropriate operations. Therefore, it is adaptable to the majority of trust propagation methods, including but not limited to the two methods presented as case studies in this paper. The topic-sensitive approach can assist in determining users' trustworthiness on different topics and facilitate human decision making when they need to take user domain knowledge into account. It can be applied in many applications, such as recommendation systems and expert finding systems, where trustworthiness and context are considered as important factors. For example, recommendation systems aim to provide accurate suggestions about different categories of products or services for users according to their preference. Topic-sensitive trust evaluation methods can boost the performance of recommendation systems by constraining the number of users, where only those suggestions provided by trustworthy users from the required domains are taken into account.

Our work can be extended in three directions. First, we plan to investigate other trust evaluation approaches for the proposed framework to build a complete system for topic-sensitive trust evaluation. Second, we will investigate how to choose an appropriate method to maximize the effectiveness of the topic-sensitive analysis according to the data characteristics. Third,



(a) PR curves of Elec (b) ROC curves of Elec

(c) PR curves of Phy (d) ROC curves of Phy

(e) PR curves of Stats (f) ROC curves of Stats

Fig. 10. PR and ROC curves of the four methods on the three topics.

trust changes over time, which makes it necessary to take the temporal aspects into account for future work.

CRediT authorship contribution statement

Xu Chen: Conceptualization, Methodology, Software, Visualization, Writing - original draft. **Yuyu Yuan:** Supervision, Funding acquisition. **Mehmet Ali Orgun:** Writing - review & editing, Funding acquisition. **Lilei Lu:** Resources, Funding acquisition.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. 91118002), the China Scholarship Council, the Australian Government through the Australian Research Council's Discovery Projects funding scheme (Project DP180102378), and the Natural Science Foundation of Hebei Province, China (No. F2019105134).

References

[1] D.M. Boyd, N.B. Ellison, Social network sites: Definition, history, and scholarship, IEEE Eng. Manage. Rev. 38 (3) (2010) 16–31, http://dx.doi.org/10.1109/EMR.2010.5559139.

[2] X. Liu, G. Tredan, A. Datta, A generic trust framework for large-scale open systems using machine learning, Comput. Intell. 30 (4) (2014) 700–721, http://dx.doi.org/10.1111/coin.12022.

[3] X. Liu, A. Datta, K. Rzadca, Trust beyond reputation: A computational trust model based on stereotypes, Electron. Commer. Res. Appl. 12 (1) (2013) 24–39, http://dx.doi.org/10.1016/j.elerap.2012.07.001.

[4] R. Guha, R. Kumar, P. Raghavan, A. Tomkins, Propagation of trust and distrust, in: Proceedings of the 13th International Conference on World Wide Web, WWW '04, ACM, New York, NY, USA, 2004, pp. 403–412, http://dx.doi.org/10.1145/988672.988727.

[5] J.H. Cho, K. Chan, S. Adali, A survey on trust modeling, ACM Comput. Surv. 48 (2) (2015) 28:1–28:40, http://dx.doi.org/10.1145/2815595.

[6] C.N. Ziegler, G. Lausen, Propagation models for trust and distrust in social networks, Inf. Syst. Front. 7 (4) (2005) 337–358, http://dx.doi.org/10.1007/s10796-005-4807-3.

[7] J. Wu, R. Xiong, F. Chiclana, Uninorm trust propagation and aggregation methods for group decision making in social network with four tuple

Please cite this article as: X. Chen, Y. Yuan, M.A. Orgun et al., A topic-sensitive trust evaluation approach for users in online communities, Knowledge-Based Systems (2020) 105546, https://doi.org/10.1016/j.knosys.2020.105546.

information, Knowl.-Based Syst. 96 (2016) 29–39, http://dx.doi.org/10.1016/j.knosys.2016.01.004.

[8] M. Ghavipour, M.R. Meybodi, Trust propagation algorithm based on learning automata for inferring local trust in online social networks, Knowl.-Based Syst. 143 (2018) 307–316, http://dx.doi.org/10.1016/j.knosys.2017.06.034.

[9] A. Rezvanian, B. Moradabadi, M. Ghavipour, M.M.D. Khomami, M.R. Meybodi, Learning Automata Approach for Social Networks, Vol. 820, Springer, 2019, pp. 241–279, http://dx.doi.org/10.1007/978-3-030-10767-3.

[10] W. Jiang, G. Wang, M.Z.A. Bhuiyan, J. Wu, Understanding graph-based trust evaluation in online social networks: Methodologies and challenges, ACM Comput. Surv. 49 (1) (2016) 10:1–10:35, http://dx.doi.org/10.1145/2906151.

[11] W. Sherchan, S. Nepal, C. Paris, A survey of trust in social networks, ACM Comput. Surv. 45 (4) (2013) 47:1–47:33, http://dx.doi.org/10.1145/2501654.2501661.

[12] M. Khani, Y. Wang, M.A. Orgun, F. Zhu, Context-aware trustworthy service evaluation in social internet of things, in: C. Pahl, M. Vukovic, J. Yin, Q. Yu (Eds.), Service-Oriented Computing, Springer International Publishing, Cham, 2018, pp. 129–145, http://dx.doi.org/10.1007/978-3-030-03596-9_9.

[13] Y. Wang, L. Li, G. Liu, Social context-aware trust inference for trust enhancement in social network based recommendations on service providers, World Wide Web 18 (1) (2015) 159–184, http://dx.doi.org/10.1007/s11280-013-0241-5.

[14] C. Jiang, S. Liu, Z. Lin, G. Zhao, R. Duan, K. Liang, Domain-aware trust network extraction for trust propagation in large-scale heterogeneous trust networks, Knowl.-Based Syst. 111 (2016) 237–247, http://dx.doi.org/10.1016/j.knosys.2016.08.019.

[15] T. Knap, I. Mlýnková, Towards topic-based trust in social networks, in: Ubiquitous Intelligence and Computing, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, pp. 635–649, http://dx.doi.org/10.1007/978-3-642-16355-5_48.

[16] Z. Gyöngyi, H. Garcia-Molina, J. Pedersen, Combating web spam with TrustRank, in: Proceedings of the Thirtieth International Conference on Very Large Data Bases, Vol. 30, VLDB '04, VLDB Endowment, 2004, pp. 576–587, http://dx.doi.org/10.1016/B978-012088469-8.50052-8.

[17] L. Lu, Y. Yuan, A novel TOPSIS evaluation scheme for cloud service trustworthiness combining objective and subjective aspects, J. Syst. Softw. 143 (2018) 71–86, http://dx.doi.org/10.1016/j.jss.2018.05.004.

[18] A. Jøsang, E. Gray, M. Kinateder, Analysing topologies of transitive trust, in: Proceedings of the First International Workshop on Formal Aspects in Security & Trust, FAST2003, Pisa, Italy, 2003, pp. 9–22.

[19] A. Jøsang, S. Pope, Semantic constraints for trust transitivity, in: Proceedings of the 2nd Asia-Pacific Conference on Conceptual Modelling, Vol. 43, APCCM '05, Australian Computer Society, Inc., Darlinghurst, Australia, Australia, 2005, pp. 59–68.

[20] J.A. Golbeck, Computing and Applying Trust in Web-Based Social Networks (Ph.D. thesis), University of Maryland, 2005.

[21] P. Avesani, P. Massa, R. Tiella, Moleskiing. it: A trust-aware recommender system for ski mountaineering, Int. J. Infonomics 20 (35) (2005) 1–10.

[22] G. Wang, J. Wu, Multi-dimensional evidence-based trust management with multi-trusted paths, Future Gener. Comput. Syst. 27 (5) (2011) 529–538, http://dx.doi.org/10.1016/j.future.2010.04.015.

[23] W. Jiang, G. Wang, SWTrust: Generating trusted graph for trust evaluation in online social networks, in: 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, 2011, pp. 320–327, http://dx.doi.org/10.1109/TrustCom.2011.251.

[24] W. Jiang, G. Wang, J. Wu, Generating trusted graphs for trust evaluation in online social networks, Future Gener. Comput. Syst. 31 (2014) 48–58, http://dx.doi.org/10.1016/j.future.2012.06.010, Special Section: Advances in Computer Supported Collaboration: Systems and Technologies.

[25] G. Liu, Y. Wang, M.A. Orgun, Optimal social trust path selection in complex social networks, in: Proceedings of the Twenty-Fourth AAAI Conference on Artificial Intelligence, AAAI'10, AAAI Press, 2010, pp. 1391–1398.

[26] G. Liu, Y. Wang, M.A. Orgun, E. Lim, Finding the optimal social trust path for the selection of trustworthy service providers in complex social networks, IEEE Trans. Serv. Comput. 6 (2) (2013) 152–167, http://dx.doi.org/10.1109/TSC.2011.58.

[27] Y.A. Kim, An enhanced trust propagation approach with expertise and homophily-based trust networks, Knowl.-Based Syst. 82 (2015) 20–28, http://dx.doi.org/10.1016/j.knosys.2015.02.023.

[28] Y.A. Kim, H.S. Song, Strategies for predicting local trust based on trust propagation in social networks, Knowl.-Based Syst. 24 (8) (2011) 1360–1371, http://dx.doi.org/10.1016/j.knosys.2011.06.009.

[29] L. Page, S. Brin, R. Motwani, T. Winograd, The PageRank Citation Ranking: Bringing Order to the Web, Tech. Rep., Stanford InfoLab, 1999.

[30] G. Wang, J. Wu, FlowTrust: Trust inference with network flows, Front. Comput. Sci. China 5 (2) (2011) 181, http://dx.doi.org/10.1007/s11704-011-0323-4.

[31] W. Jiang, J. Wu, F. Li, G. Wang, H. Zheng, Trust evaluation in online social networks using generalized network flow, IEEE Trans. Comput. 65 (3) (2016) 952–963, http://dx.doi.org/10.1109/TC.2015.2435785.

[32] M.H. Jang, C. Faloutsos, S.W. Kim, U. Kang, J. Ha, PIN-TRUST: Fast trust propagation exploiting positive, implicit, and negative information, in: CIKM, ACM, 2016, pp. 629–638, http://dx.doi.org/10.1145/2983323.2983753.

[33] M. Ghavipour, M.R. Meybodi, A dynamic algorithm for stochastic trust propagation in online social networks: Learning automata approach, Comput. Commun. 123 (2018) 11–23, http://dx.doi.org/10.1016/j.comcom.2018.04.004.

[34] B. Wu, V. Goel, B.D. Davison, Topical TrustRank: Using topicality to combat web spam, in: Proceedings of the 15th International Conference on World Wide Web, WWW '06, ACM, New York, NY, USA, 2006, pp. 63–72, http://dx.doi.org/10.1145/1135777.1135792.

[35] F. Sebastiani, Machine learning in automated text categorization, ACM Comput. Surv. 34 (1) (2002) 1–47, http://dx.doi.org/10.1145/505282.505283.

[36] Y. Zhang, G. Zhang, H. Chen, A.L. Porter, D. Zhu, J. Lu, Topic analysis and forecasting for science, technology and innovation: Methodology with a case study focusing on big data research, Technol. Forecast. Soc. Change 105 (2016) 179–191, http://dx.doi.org/10.1016/j.techfore.2016.01.015.

[37] H. Ghiasi, M. Fathian Brojeny, M.R. Gholamian, A reputation system for e-marketplaces based on pairwise comparison, Knowl. Inf. Syst. 56 (3) (2018) 613–636, http://dx.doi.org/10.1007/s10115-017-1141-2.

[38] D.M. Blei, A.Y. Ng, M.I. Jordan, Latent Dirichlet allocation, J. Mach. Learn. Res. 3 (2003) 993–1022, http://dx.doi.org/10.1162/jmlr.2003.3.4-5.993.

[39] D.M. Blei, Probabilistic topic models, Commun. ACM 55 (4) (2012) 77–84, http://dx.doi.org/10.1145/2133806.2133826.

[40] G. Zhou, J. Zhao, T. He, W. Wu, An empirical study of topic-sensitive probabilistic model for expert finding in question answer communities, Knowl.-Based Syst. 66 (2014) 136–145, http://dx.doi.org/10.1016/j.knosys.2014.04.032.

[41] C.-K. Yau, A. Porter, N. Newman, A. Suominen, Clustering scientific documents with topic modeling, Scientometrics 100 (3) (2014) 767–786, http://dx.doi.org/10.1007/s11192-014-1321-8.

[42] Y. Zhang, H. Chen, J. Lu, G. Zhang, Detecting and predicting the topic change of Knowledge-Based systems: A topic-based bibliometric analysis from 1991 to 2016, Knowl.-Based Syst. 133 (2017) 255–268, http://dx.doi.org/10.1016/j.knosys.2017.07.011.

[43] D. Ramage, D. Hall, R. Nallapati, C.D. Manning, Labeled LDA: A supervised topic model for credit attribution in multi-labeled corpora, in: Proceedings of the 2009 Conference on Empirical Methods in Natural Language Processing, Vol. 1, EMNLP '09, Association for Computational Linguistics, Stroudsburg, PA, USA, 2009, pp. 248–256, http://dx.doi.org/10.3115/1699510.1699543.

[44] L. MacLeod, Reputation on stack exchange: Tag, you're it!, in: 2014 28th International Conference on Advanced Information Networking and Applications Workshops, 2014, pp. 670–674, http://dx.doi.org/10.1109/WAINA.2014.108.

[45] T. Cleff, Exploratory Data Analysis in Business and Economics, first ed., Springer, 2014, pp. 88–92, http://dx.doi.org/10.1007/978-3-319-01517-0.

[46] J. Davis, M. Goadrich, The relationship between precision-recall and ROC curves, in: Proceedings of the 23rd International Conference on Machine Learning, ICML '06, ACM, New York, NY, USA, 2006, pp. 233–240, http://dx.doi.org/10.1145/1143844.1143874.

[47] S. Shekarpour, S. Katebi, Modeling and evaluation of trust with an extension in semantic web, J. Web Semant. 8 (1) (2010) 26–36, http://dx.doi.org/10.1016/j.websem.2009.11.003.

Please cite this article as: X. Chen, Y. Yuan, M.A. Orgun et al., A topic-sensitive trust evaluation approach for users in online communities, Knowledge-Based Systems (2020) 105546, https://doi.org/10.1016/j.knosys.2020.105546.