JOURNAL OF EXPERIMENTAL & THEORETICAL ARTIFICIAL INTELLIGENCE, 2017
VOL. 29, NO. 3, 537–556
http://dx.doi.org/10.1080/0952813X.2016.1199601

Taylor & Francis
Taylor & Francis Group

Trust estimation of the semantic web using semantic web clustering

Hossein Shirgahi[a], Mehran Mohsenzadeh[a] and Hamid Haj Seyyed Javadi[b]

[a]Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran; [b]Department of Mathematics and Applications, Shahed University, Tehran, Iran

ABSTRACT

Development of semantic web and social network is undeniable in the Internet world these days. Widespread nature of semantic web has been very challenging to assess the trust in this field. In recent years, extensive researches have been done to estimate the trust of semantic web. Since trust of semantic web is a multidimensional problem, in this paper, we used parameters of social network authority, the value of pages links authority and semantic authority to assess the trust. Due to the large space of semantic network, we considered the problem scope to the clusters of semantic subnetworks and obtained the trust of each cluster elements as local and calculated the trust of outside resources according to their local trusts and trust of clusters to each other. According to the experimental result, the proposed method shows more than 79% Fscore that is about 11.9% in average more than Eigen, Tidal and centralised trust methods. Mean of error in this proposed method is 12.936, that is 9.75% in average less than Eigen and Tidal trust methods.

ARTICLE HISTORY
Received 20 September 2015
Accepted 21 February 2016

KEYWORDS
Trust estimation; semantic web; clustering; social network

Introduction

A social network is a group of people, organisation or other social entities that are related by a series of social relationships, such as friendship, cooperation or information exchange. Web is an example of a social network. Social networks are formed by connecting web pages. Web can be considered as a graph that its vertices are web pages and the edges are the hyperlinks. While the web pages may be in a concept similar to a text or multimedia files, a hyperlink is usually a clear indicator that web author believes it is linked to another page (Jamali & Abolhassani, 2006). There are various ways through which social network can automatically be directed to the web. Users are connected to each other via transactions in online auctions and electronic markets.

Recently, the number of virtual communities including web-based social networks has been growth rapidly. By creating and developing these web networks, many interactions have been done based on social criteria between users. This is a new way of interaction challenging issue. On the other hand, several different types of relationships between entities (humans and agents) could be the concluded in semantic web. A particular network can be made by derivation of each of these relationships (Golbeck, 2005).

Semantic web as information space that is designed with the aim of being useful not only for human–human relationship, but also to make relations that machines have the ability to participate and contribute (Berners Lee, Handler, & Lassila, 2001). For example, FOAF is a semantic web project that defines the predicate relations everywhere each user is aware of who he (she) knows (FOAF, 2000–2015). In

CONTACT Mehran Mohsenzadeh ✉ mohsenzadeh@srbiau.ac.ir

these networks, the nodes are people and the edges between the nodes show the friendship between two connected nodes in network (Lassila & Swick, 1999; W3School, 2010).

The highest level of pyramid in semantic web structure is dedicated to trust management and the last layer is allocated to the trust ability. It is important to distinct between trustworthy information and unreliable information on the web (Golbeck & Hendler, 2004; Golbeck, Parsia, & Hendler, 2003).

The user must choose authoritative information based on the information he recognise is reliable. The problem is deeper when we introduce web services. Because users are forced to scrimmage a new set of requirements to rely on web services and also the web services require automated methods to trust each other.

Access to wide variety of services and resources highlights the need of trust management in semantic web.

Golbeck developed a FOAF project that shows the trust numbers in 1–9 in which 1 is absolute distrust and 9 is full trust to the people who claimed (Golbeck et al., 2003).

When users make a statement on the semantic web, they can interpret the trust by using sentence information. Subsequently, to a particular concept of trust assertion, the trust networks will be created.

A scheme proposed in Ceravolo, Damiani, and Viviani (2005) called RDF, allows users to show their trust metadata. By creating ontology languages such as OWL, it is possible to infer strongly on semantic web. Trust has different meanings and it can be seen in different views. For example, it can be considered as security and access control in computer networks, and in distributed systems it means trust and in game theory and policy it is considered as an appropriate decision in uncertain conditions.

Trust is a central part of the semantic web. In all categories of semantic web, the trust layer is to understand and accept the rules, logic, ontology science and the lower layers. Trust often refers to a mechanism to review and investigate the resource of the information to understand the authenticity of a resource.

Web slogan "anyone can say anything", makes it as a unique resource of information. In semantic web, machine must have the power of reasoning in order to estimate the authority of each information resources based on a set of criteria and also it should distinguish valid resources of information from invalid one. Another important role of trust in semantic web is to be available as a representative and automated reasoning when alternative resources of information are available and it needs to make judgments and beliefs regarding trust. The computers will be in challenge for selecting the appropriate resource because of diversity of resources quality. Also determining the authority of such diverse resources will cause problems for them.

A trust policy is used in Almendra and Schwabe (2006) which contains a set of rules that trustee use it for trust test. Various agents may exert different policies. A trust decision is a test action of a claimed fact to satisfy the trust policy or trust criteria. In fact, in some cases, there is a reservoir of trust layer that adopts a decision on the authority. An example of this system is trust mechanism used for trust emails (Ceravolo et al., 2005; Golbeck & Hendler, 2004). Trust email is a policy where a network of friends will exchange a list of emails to avoid spam without compromising each other's privacy.

In this paper, trust considered as a measurable belief that is calculated based on social network authority, authority of links pages values and semantic authority. Here a trusty decision can be considered as a transient process, as there is a web trust network so that the relationship between two entities means a trusty adopted decision and the quality value of that trust is evaluated. The absence of any correlation between any pair of entities in the network means that a trusty decision has not been taken previously.

Web trust network maybe extracted from a social network where the trust value between nodes is dedicated by the users directly. It can also be made of trust assertions in the semantic web. There are two main differences between these two networks. First, the trust value in social network does not depend on the concept. Secondly, if the expressions are shown in terms of a particular concept in semantic web, a trust network will be made based on that concept (Shekarpour & Katebi, 2010). It is also possible that the trust value between the nodes can be calculated by the values of links pages and the logical explicit parameters between the nodes. In all three states, the aim is evaluation of trust ratio

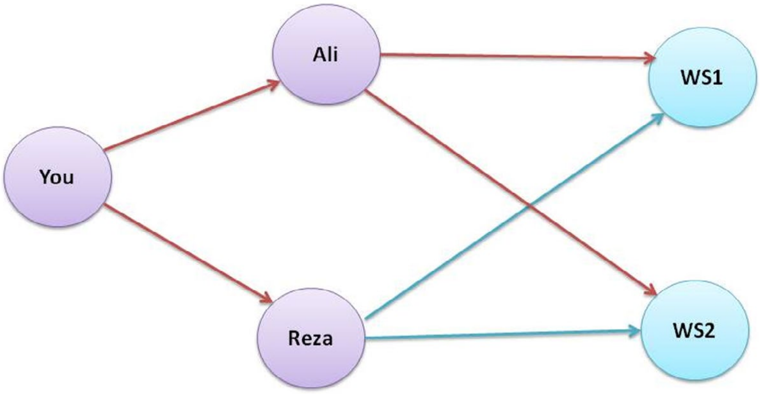

Figure 1. Scenario of evaluating the trust between entities.

between the nodes in a web trust network. Because of the breadth of web, most transactions are done in an indirect manner. If a user wishes to estimate the trust of information resources of an anonymous web site which has had no access to it and no information of trust in its history yet, the trust of this web site should be estimated based on the others knowledge from this web site.

The following scenario is an example that can be used to illustrate some concepts of this research. In this paper, an agent collects metadata from different resources and decides what metadata can be trusted.

You want to find a professional image editing software that have advanced features and be easy to use. WS1.COM website offers adobe Photoshop software but WS2.COM website offers Corel Draw software. Now, if you don't have any information about these two websites, you cannot blindly trust the information. In this case you must first build a subgraph that reflects the way that connects you to the websites.

As illustrated in Figure 1, these paths can be extracted on the semantic web through the metadata in the field of professional image editing software that is published between you and the websites WS1, WS2. For example, you know Ali and Reza in professional image editing software and they stated about the trust value of WS1, WS2 websites. The graph includes the paths that show trust value between two nodes on each edge.

Then we should calculate the trust value from you to the websites that have stated these information resources based on the graph. In this step, the evaluation agent should apply an algorithm to develop and collect and eventually assess the trust values that can be suggested to take decisions on resource.

Of course, there are a lot of challenges in this field because the trust of each of these websites can be calculated based on any of the social network authority parameters, the authority of pages links values and semantic authority that use one of these parameters which has a greater impact on user's request. One of the main features of this research is trust calculation solution, due to the fact that the relationship of trust is known as only a small portion of implications of accession on the web. On the other hand, the number of pages, users and services on the web is much larger than that needed to estimate how much trust exists between the entities. Routes connecting the entities on the network (peer to peer network, social network and semantic web network) include the information that can be used to infer how much the entities may trust to each other. On semantic web, the paths between the entities can be inferred by the interpretation of trust assertions in a certain concept.

Previous works

There are several algorithms for computing the trust on web trust network and they consider different parameters and different decision methods for calculation.

In this section, we will review the popular algorithms for calculating the trust briefly. Empirical and practical studies carried out on trust show that social interactions or online transactions are created based on trust and reputation of participations or online environment (Jarvenpaa, Tractinsky, & Vitale, 2000; Turel, Yuan, & Connelly, 2008). So a trust mechanism is needed to predict the trust about other participations and propose the trusty participations to facilitate social interactions among them. For this purpose, technical and computational trust models have been proposed in various online environments. One of the main methods of trust prediction models is global trust, like a famous model, ebay.com global trust models calculate a global value of trust for private user which uses the feedback of all visitors or a connection structure in online communities to calculate global value of trust. Kamvar et al. proposed an Eigen trust algorithm for calculating a unique global trust value for each pair of peer-to-peer file sharing network that works based on a history of files loading by each pairs that detect trust of all pairs with a model of web page ranking (Kamvar, Schlosser, & Molina, 2003).

Although many methods based on Eigen trust produce a ranking of trust among the network users, but they cannot produce trust values rating on a scale similar to that used by the users. Chin and Singh developed a complex ranking system for online communities based on ranking that provide a measure of fame for voters and produce high-quality information about the purpose of the ranking. The value of global trust (i.e. reputation) or ranks is assigned to each peer in a network, and trust value of system is quantitative measured as a whole place in each peer (Chen & Singh, 2001).

The global trust can make a clear reflection of a global agreement based on a user. Of course, it is challenging to compute the global trust values for users who receive trust values of users who give them different high and low scores as trust values.

Next method is a local trust model that is sometimes called private reputation. It computes private trust value as a subjective point of view for each network users.

Some researchers consider only the local trust as correct criteria and they recognise the global trust from these them. They claim to define local trust as a trust and global trust as a reputation. With this assumption the user clearly has identified a small set of users who trust them and then defines a private trust if exists. The trust of a user to an unknown user is measured based on a series of communications of direct trust around the users and a series of communications of indirect trust that are available by passing a set of trust chains.

Richardson et al. have provided trust prediction mechanisms based on trust propagation in web of trust including continuous trust values. Trust value of a source user to destination user is measured by trust propagation through a trusted user network to achieve a destination user (Richardson, Agrawal, & Domingos, 2003).

Guha et al. developed a trust propagation framework that measures the distribution of the web of trust by introducing some concepts such as co citation, transpose trust and trust coupling and then propagates the trust and distrust (Guha, Kumar, Raghaven, & Tomkins, 2004). The performance of such trust propagation methods cannot help being influenced by the density of web trust. If a web of trust is a very sparse, it will be difficult to find trusty paths by the user from a source user to a destination user. Cumulative functions in each probability trust chain of recourse user to a destination user affects on accuracy of prediction. Computational complexity of aggregation grows exponentially in trust propagation method. As there are number of available users and many different paths with different lengths. They benefited the idea of distrust transitivity and spread trust propagation and computational behaviour of distrust propagation. He also used Epinions network to test, as data have discrete values from +1 to −1 to trusty links and distrust links, respectively.

Matsuo and Yamamoto empirically measured the mutual trust and products similar rankings in a common community of collective review of Japanese ornamental products. In this paper, they identified positive features through the development of a trust prediction model of SVM classifier, like common trust neighbouring and similarity of common products ranking among users (Matsuo & Yamamoto, 2009).

Zolfaghar and Aghaieb have shown a time-aware trust prediction method that offers prediction of relationships or trust future connections using learning method through interim assessment. As long as most recent studies about trust prediction use trust graph structure in a single moment, time-aware trust prediction effect on dynamics of trusted networks and then accuracy of predicting trust connections will be improved in future (Zolfaghar & Aghaie, 2011). The growing research on trust in social networks established a growing interest in recommender systems based on trust. Such systems combine trust relationships among the users with the recommended algorithms that trust information are used as a complex filter to find a suitable neighbour. One of the most important features in recommender systems that improve trust is increasing trust propagation mechanism.

Compared to the traditional proposed systems that have been applied collective filtering, this approach improved the performance of suggestions. Pitsilis and Chia studied whether the explicit trust relationships can improve the efficiency of suggestions in user relationships in trust network (Pitsilis & Chia, 2010). They found that using explicit trust to find best neighbour is much useful than recent active users who are less experienced than active users in Epinions data-set.

Yuan et al. identified the characteristics of small words in explicit trust networks. Then these features were used to improve the recommender systems that improve trust (Yuan, Guan, Lee, Lee, & Hur, 2010). O'Donovan and Smyth and Victor et al. have focused on a simple and useful method as compared with proposed standard algorithms instead of using explicit trust information and the level of trust are simply measured by ranking on reviews (O'Donovan & Smyth, 2006; Victor, Cornelis, Cock, & Teredesai, 2008). O'Donovan and Smyth have measured the user trust, based on a history of ranking errors related to the offers. This error-based trust model is a global trust that affects the companies of all users (O'Donovan & Smyth, 2006).

Victor et al. simply have defined the key modes like skilled person, repetitive ranks and connectors based on a written review or ranking. These selected key modes are famous users that have rated and written most of reviews and items. It also provides a global trust but it cannot be very effective on making private offers to users who have different priorities (Victor et al., 2008).

Kim and Phalak predicted the trust rate without using explicit trust rankings that are not always available and also collecting them in sufficient quantities to predict trust is difficult. In addition, the produced trust value by this model uses the same parameters which are used by the users to assign the rankings not a single rank or dependent rank (Kim & Phalak, 2012).

Therefore, when they have been available to improve the density of web of trust, the estimated trust value can be added to explicit trust values. Dense web of trust provides a chance to improve some application, like a recommended system of trust propagation for users that are far apart.

Golbeck has provided a comprehensive review of web of trust. The author considers three areas for trust: trust in content, trust in services and trust in public. It is said that trust in content has two parts as trust to web pages and trust to semantic web information resources. When the users see the websites, they should decide whether the web content is reliable or not (Golbeck, 2006a). Some factors affect the user about the website authority, website design, activities, links, political assertions and owners external authority that impact the trust. On the other hand, using semantic web techniques we can present the origin. Resource is defined as a data history. Knowledge about the recourses helps the users to review the accuracy of data and decide about trustiness. In fact, the interconnection of data is important to judge about the data quality. Users may be able to make judgments about the value of trust content by the resources.

Trust in services means specifying and a two-way trust management or services, which require a system that can control and scale the distributed nature of entity. Trust management models explain how trust information is stored and how it is shared in peer-to-peer network. If each node informs the data about its interaction to all, it adds huge overhead to network and hence, each node allocates a trust value to the nodes that has direct access to them. When a node wants to discover a value of an unknown node, it releases a request for information; subsequently the neighbours will extend the request to reach a given time. Once the data about a node are collected, this information should be combined to form a recommendation and determine trust value to a node. Finally, trust in public is based on the stored values of trust in social networks. Web-based social networks maintain trust values and provide an interaction point where it can be assembled and be available. For human interaction, trust is always an important relationship. In semantic web and web, social network is becoming an important relationship by FOAF. Many people have accounts on multiple social network websites. If a website builds FOAF profiles for its users, it allows the users to have their data. Instead of having locked data in a private database, they can share information or connect to it. The main features of web-based social networks are portability, synchronisation, privatisation and content. When two people know each other, they know how much they can trust each other. Two people, who are not directly connected, do not have a base to understand trust. Although their connecting path in web contains information that can be used to guess how much they can trust each other.

In another report, Golbeck has focused on trust in social networks and derived characteristics from real networks graphs and proposed an algorithm called Tidal trust for inferring trust that rely on trust graphs (Golbeck, 2006b).

Richardson et al. used a trust network to calculate the belief of user to an expression. Calculation is based on the path from the resource to each node that offers an idea about the expression; he integrates trust values to calculate final trust value about the expression. This method is statistical interpretation similar to a random walking on a Markov chain. He used Epinions network to test their algorithm and evaluate the results (Richardson et al., 2003).

Chen et al. focus on large-scale mobile social networks to solve the problem describing user trustworthiness because of overlapping of users between more than one communities or clusters. They propose an algorithm called *k*-Fuzzy Trust by creating a fuzzy virtual social graph under fuzzy degree *k* simulation between mobile users according to static attributes and dynamic behavioural patterns (Chen, Wang, & Jia, 2015).

Shafiq et al. have proposed their method of finding the preferences of users from the related sections of their social networks and communities by discovering the users' operations in their social networks, and also related information from users' social networks, according to their proposed trust and related matrices (Shafiq, Alhajj, & Rokne, 2015).

Tang et al. propose a framework of evolution trust, eTrust, which exploits the dynamics of user preferences in the context of online product review. They present technical details about modelling trust evolution, and perform tests to show how the exploitation of trust evolution can help improve the performance of online applications such as rating and trust prediction (Tang, Gao, Liu, & Sarma, 2012).

Ziegler and Lausen offered a trust algorithm called Appleseed. It is owned by a local group of trust calculation which is compared with Advocate group. Trust metrics of local group means calculating neighbourhood of trust and return rankings of all nodes in the network by receiving network and a resource. Global metrics require a thorough knowledge of entire trust network. Also a discussion of the semantics and propagation models of distrust are provided (Ziegler & Lausen, 2005).

Lesani and Bagheri used a fuzzy model to evaluate the trust and compared it with Tidal trust (Lesani & Bagheri, 2006). This Algorithm used fuzzy variables to determine the trust among users and offered a technique for trust between two nodes that may not be directly related in social network graph. Sabater and Sierra offered a research in field of computational mechanisms for trust in virtual communities (Sabater & Sierra, 2005).

Classification of trust models

There are several trust models in semantic web (Linn et al., 2004). Different models and policies can be classified based on different analytical approaches and node interactions. If one node needs trust value of an anonymous node, How it can interact with the community? Can it trust to all? Or should it choose a node that is trusty for getting information? In this case How it should select? In general, there are two categories of trust models. The first model has centralised structure and administrator or central node is responsible for trust management in web trust. The second model has a distributed structure and tries to request a node that trusts it directly or it is available through trusty nodes. Distributed trust models are classified as global or local.

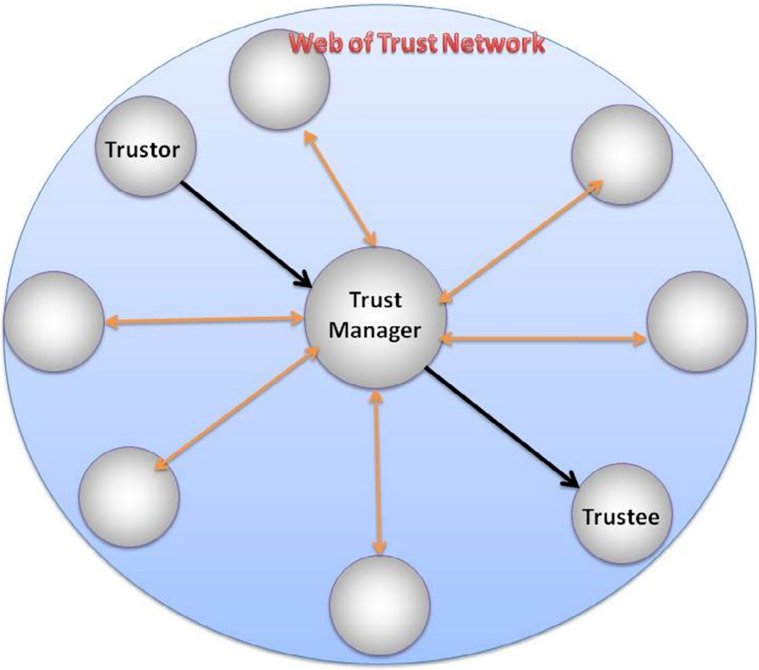

Figure 2. Centralised trust model.

Centralised trust model

A centralised node acts as a system administrator. This administrator needs knowledge such as trust value and nodes histories. The administrator also can judge the nodes and applies system policies as some criteria or rule sets. When a source node needs to interact with the other destination node, it asks the manager if it can trust destination or not. So there is no clear trust model among the nodes. A node can only communicate with the centralised node to gather information about another nodes trust. This structure is shown in Figure 2. The administrator gathers information from both parties involved in interaction. Some of the major problems with this model are how a person can trust the administrator node, or how nodes trust each other and linked. Also this model has no high scalability. In fact, one can never have a comprehensive system that knows and trust everyone.

Distributed trust model

In this model, there is no centralised system to control the trust. The nodes are responsible for obtaining mutual trust according to their direct interaction. There is no global trust. If node A wants to know the trust of node B, it should want the other nodes to evaluate node B. Then the values that others give to B are combined to calculate the B trust. This model is shown in Figure 3. The distributed models can be divided into two categories: global and local. Global models calculate global trust for each node of the network. Regardless of who has requested a recommendation of the trust, always the same answer is given. Local trust models calculate the trust in response to the need of a node to recommended trust and the results for each node becomes private (Golbeck, 2005).

Global trust model: this model is based on the degree of node propagation in community. The neighbours of a trusty type know it because of its past relations. A node may interact with neighbours in past and neighbours have profiles of this node's history. According to the neighbours' ideas, one person may vote for being trusty or distrust. Voting is an example of evaluation of trust value. But this

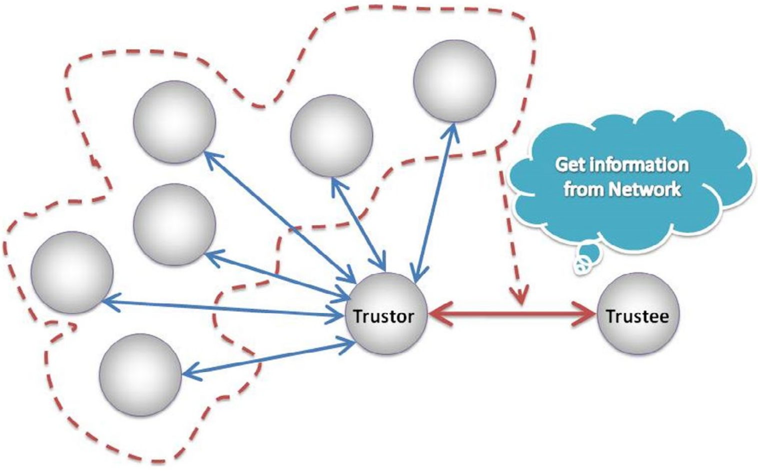

Figure 3. Distributed trust model.

method suffers from the problem that giving information and being unaware are combined on the web to some extent.

It is easy for a user or many users to gather several people to show lots of their prejudices ideas. www.ebay.com and www.amazon.com have a special trust mechanism. Both of them have been used as centralised ranking models which manage the trust of any user. But on the other hand, authority calculation is according to the global approaches that depend on user ranking. Because of the problems with previous methods, one may ask the only opinions about the nodes which are valid. Clearly, the information obtained from these nodes is much trustier. Now the problem is what defines a valid node. A valid node is defined based on characteristics and performance of the system. One criterion might be that a node that has high criterions of social networks can be a valid node (e.g. a node that has a large number of edges). HTS algorithm is a link analysis algorithm that ranks the web pages because of their authority features and ranks hub values to determine the authority of web pages (Kleinberg, 1998).

The trust value evaluates the value of page content and the value of hub determines the value of a page links to other pages. These values can be used for ranking web search results. The hub value and the authority are defined interchangeably. The authority value is calculated as a form of collective of hub values as scaled which refers that page. A hub value is total amount of scaled authority of the pages pointing to it. Each *u* node is initialised as 1 with *a* and *h* scores in an extension graph (Equation (1)). Then HITS is specified iteratively. $\sum_u h\, u$ and $\sum_v av$ are normalised to 1 and will be converged after some iterations (Kleinberg, 1998).

$$a_u = \sum_{u \to v} h_u,\ h_u = \sum_{v \to u} a_u \tag{1}$$

We can use hub value and authority to evaluate the trust. If a node trusts trusty nodes, it will be a good hub and if trusty node trusts it, it will be used as a good resource. Anyway, these values are used in trust ranking. Page rank in Google is like HITS that searches the results to make a ranking for web pages and is a link analysis algorithm which assigns a numerical weighting to each element of hyperlink documents to measure the relative importance of this group (Page, Brin, Motwani, & Winograd, 1998).

Eigen trust algorithm (Kamvar et al., 2003) can be used in peer-to-peer systems and computes the trust with some types of page rank algorithms. In Eigen trust algorithm, trust is a performance scale.

Local model: in this model, trust is private and the belief of two people is different and privatisation should improve the accuracy of results. Most of report researches (Golbeck, 2005) in trust mechanisms of semantic web review the algorithms that calculate trust in private view.

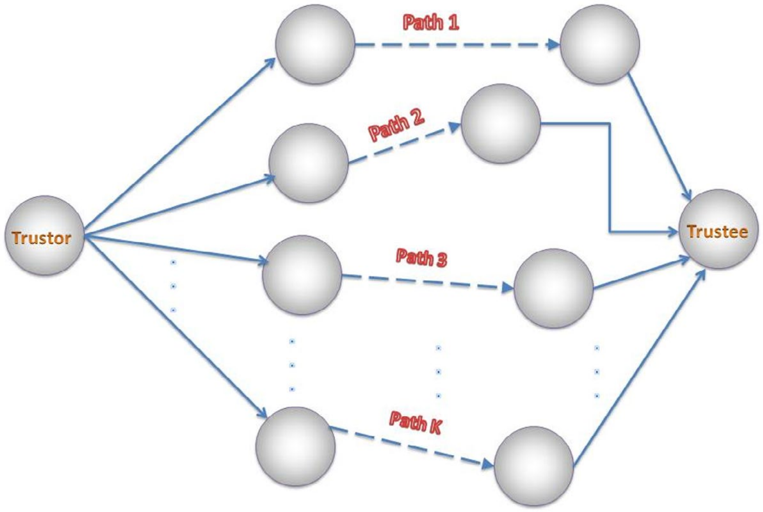

Figure 4. A sample of K different paths between trustor and trustee nodes.

If someone does not know the trusty, his friends or friends of friend may know it. The main idea here is that anyone would trust his friend's belief more than other strangers' belief. A trusty friend believes his friends' beliefs and it is possible to find a path between who trusts and trustee. According to small world theory (Milgram, 1967), each pair of nodes in a random network will be connected by a short chain of random acquaintances. The number of interfaces is limited, so the person who trust and trustee are connected by less than 6 interval nodes. This implies that if such a chain of mutual acquaintance is used to determine the initial trust between each pair of entities, then the method is well scaled, because these chains tend to be short. The main problem here is calculating the trust values between unknown entities.

In this paper, we used a semantic web network clustering model to take advantage of the benefits of both centralised and distributed models.

Clustering model for trust estimation

Before describing the clustering model for trust evaluation in semantic web, first we describe the parameters used in this paper to assess the trust. We used the parameters of the social network authority, authority of pages links values and semantic authority. We can consider different parameters to assess the trust in semantic web. To increase users satisfaction, it is very effective to consider social network criteria, because semantic criteria do not completely conform to social networks criteria in many demands and users tendency is more based on social networks criteria. In this paper, the authority of the social network is amount of explicit authority that nodes announce directly to each other based on a set of statements or assertions. However, if there is no explicit authority between two nodes as direct ideas, it should be calculated from neighbouring nodes indirectly and inductively. Figure 4 shows an example of an indirect relationship between the two nodes of trustor and trustee in semantic web that are linked through indirect *K* different paths to each other. In this case, the authority of social network in each path should be obtained based on Equation (2). Then the authority of the trustee node in social network is given by Equation (3).

$$\mathrm{SNAP}(i, S, D, \mathrm{Data}) = \left(\prod_{j=S}^{D-1} \mathrm{SNAN}(j, j+1) \right) \times \mathrm{SNAD}(D, \mathrm{Data}) \tag{2}$$

In Equation (2), the parameter SNAP (i, S, D, DATA) is the social network authority of path i where S is the source node (trustor) and D is the destination node (trustee) and DATA is a data that the trustee node has identified for a direct authority of social network that has been showed by SNAD (D, Data) in this equation. Every path from node S to D is a set of nodes in a social network where each node is neighbour of next node in this path and neighbours' nodes identified their social network authority directly which is shown by SNAN ($j, j+1$) in Equation (3). Since all SNAN and SNAD values are in range [0, 1] the value of social network authority in each path will be in range [0, 1].

$$\mathrm{SNA}(S, D,\ \mathrm{Data}) = \max(\mathrm{SNAP}\ (i, S, D,\ \mathrm{Data})\ \text{for every path}\ i = 1\ \text{to}\ k) \tag{3}$$

In Equation (3), SNA(S, D, Data) identifies the authority of social network trustee node D to the trustor node S for Data information, that if there are K different paths from node S to node D, authority of that social network will be the most reliable social network between these K paths.

One of the criteria that have a great impact on evaluating the trust of web network is the value of websites reputation that can be estimated by visiting them, especially the number of links to these pages or some other communication parameters of web networks. Usually nodes that are more generally known are more trusted. In this paper, we used authority of pages links value to get a reputation and we use parameter h in HITS algorithm to obtain it (Kleinberg, 1998). Of course when there is no authority of pages links value between two nodes directly, it must be calculated indirectly and inductively from neighbouring nodes. Like Figure 4 that shows relationship between two nodes of trustor and trustee in the semantic web that are linked through K different paths indirectly, in this case we should obtain the authority of pages links value for each path based on Equation (4). Then we can obtain the authority of pages links value of trustee node based on Equation (5).

$$\mathrm{NLAP}(i, S, D, \mathrm{Data}) = \left(\frac{\sum_{j=S}^{D-1} \mathrm{NLAN}(j, j+1)}{D - S} \right) \times \mathrm{NLAD}(D, \mathrm{Data}) \tag{4}$$

In Equation (4), parameter NLAP (i, S, D, Data) is the of pages links value in path I that its trustor node is S and its trustee is D and Data is a data that a trustee node identified a authority of direct pages links value that is identified by NLAD (D, Data) in this equation. Every path from node S to node D consists of set of nodes in web network that each node is neighbour with the next node in the path and neighbour's nodes have identified the authority of each other pages with parameter h in HITS algorithm directly. Here, it is shown by NLAN ($j, j+1$). Since all NLAN and NLAD values are in [0, 1] range, the authority of pages links values of each path will be in the [0, 1] range too.

$$\mathrm{NLA}(S, D, \mathrm{Data}) = \frac{\sum_{i=1}^{K} \mathrm{NLAP}(i, S, D, \mathrm{Data})}{K} \tag{5}$$

In Equation (5), NLA (S, D, Data) identifies the authority of pages links values of trustee node D to trustor node S for data information. If there is K several paths from node S to node D, the authority of the pages links value will be the average of pages links values of these K paths. In semantic web networks, the most important criterion for evaluating network trust is semantic authority. Semantic authority in semantic web nodes is calculated according to information resources that nodes express during the time and their ranks in different categories of semantic web networks. Experimentally, usually the nodes have more authority in a specific area can be more trusted in that area. Each node can determine directly the semantic authority of its neighbouring nodes in any request based on metadata that it has in its history. However, when there is no semantic authority between two nodes directly, it must be calculated indirectly from its neighbouring nodes. Such as Figure 4 that show an indirect relationship between two trustee and trustor nodes in semantic web that are connected through indirect different K paths. In this case, at first, the semantic authority of each path must be achieved by means of Equation (6) and then semantic authority of trustee node is given by Equation (7).

$$\mathrm{SAP}(i, S, D, \mathrm{Data}) = \left(\prod_{j=S}^{D-1} \mathrm{SAN}(j, j+1) \right) \times \mathrm{SAD}(D, \mathrm{Data}) \tag{6}$$

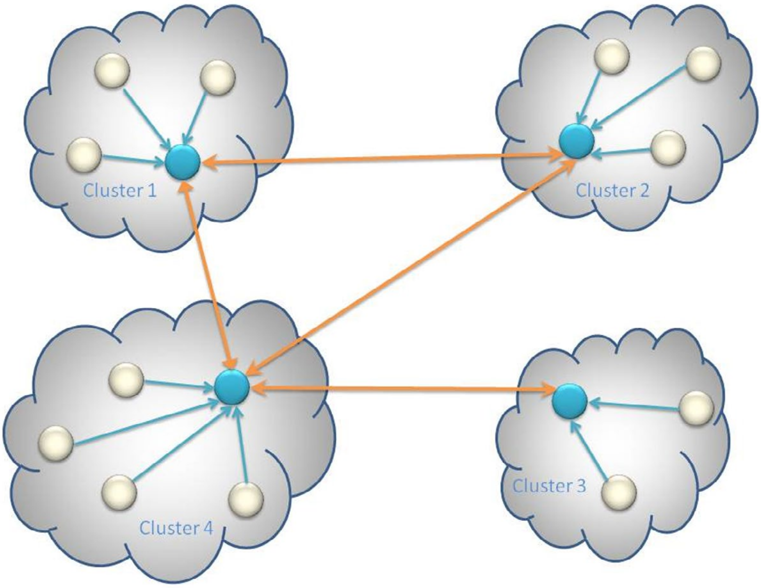

Figure 5. A sample of cluster structure of web trust network.

In Equation (6), the parameters SAP (*i*, *S*, *D*, Data) is a semantic authority of path *i* that its trustor node is *S* and its trustee node is *D* and Data is information that trustee node of a semantic authority has identified for it and is shown by SAD (*D*, DATA) in this equation. Every path from node *S* to *D* consists of set of nodes in the semantic web network that every node is neighbour to the next node in this path. And neighbour nodes has identified each other's semantic authority directly, that is shown in this equation as SAN (*j*, *j* + 1). Since all SAN and SAD values are in [0, 1] range, the semantic authority of each path will be in [0, 1] range.

$$\mathrm{SA}(S, D, \mathrm{Data}) = \max(\mathrm{SAP}(i, S, D, \mathrm{Data})) \text{ for every path } i = 1 \text{ to } k \tag{7}$$

In Equation (7), SA(*S*, *D*, Data) specifies semantic authority of trustee node *D* to trustor node *S* for Data information that if there are *K* different paths from node *S* to node *D*, that semantic authority will be the greatest semantic authority between these *K* paths.

Trust is calculated based on combination of parameters such as social network authority, authority of pages links value and semantic authority according to the Equation (8).

$$\begin{cases} T(S, D, \mathrm{Data}) = \alpha \mathrm{SNA}(S, D, \mathrm{Data}) + \beta \mathrm{NLA}(S, D, \mathrm{Data}) + \gamma \mathrm{SA}(S, D, \mathrm{Data}) \\ \alpha + \beta + \gamma = 1 \end{cases} \tag{8}$$

In Equation (8), *T* (*S*, *D*, Data) is trust and *α*, *β* and *γ* are determined based on user request and importance of social network authority parameters, authority of pages links value and semantic authority.

In real world, internet development caused very broad semantic network space, also, in addition to physical expansion; diversity in types of subjects in semantic network is another challenge. In order to solve these problems in this paper, the problem space is divided into clusters of semantic subnetworks (Figure 5) and we obtained trust elements of any cluster locally. It means if trustor and trustee nodes of a request existed in one cluster and they have no direct access to each other, by considering semantic network space in one cluster we can calculate the trust by means of Equation (8), but if the trustee and trustor nodes were in separated clusters, first the authority of trustee node than its cluster head is calculated based on Equation (8). Then authority of trustor and trustee nodes is calculated than each other. If two clusters were neighbours, they have each other's trust in their history, if they were not neighbours, cluster trust must be calculated indirectly by means of access paths which is calculated by neighbour clusters in web trust network. For this, at first we calculate clusters trust in each path by means of Equation (9) and then according to Equation (10), if different *K* paths existed between two trustee and trustor nodes clusters, a path with higher trust is determined as their cluster trust and finally trust of trustor node to trustee node is obtained based on Equation (11).

$$\mathrm{CLTP}(i,\mathrm{CS},\mathrm{CD}) = \prod_{i=\mathrm{CS}}^{\mathrm{CD}-1} \mathrm{DCLT}(j,j+1) \tag{9}$$

In Equation (9), CLTP (*i*, CS, CD) parameter is cluster trust of path *i* that its trustor cluster head is CS and its trustee cluster head is CD. Any path from CS node to CD node consists of a set of cluster heads in semantic web network that any node is neighbour of the next node in this path and neighbour nodes directly determine their cluster's trust which is shown by DCLT(*j*, *j* + 1) in this equation. While all DCLT values existed in the [0, 1], cluster trust value of any path will be in [0, 1].

$$\mathrm{CLT}(\mathrm{CS},\mathrm{CD}) = \max(\mathrm{CLTP}(i,\mathrm{CS},\mathrm{CD})) \text{ for every path } i = 1 \text{ to } k \tag{10}$$

In Equation (10), CLT (CS,CD) is cluster trust that determines CS trustor cluster end for CD trustee cluster head and if *K* different paths existed from node CS to node CD, the path with higher trust is determined as their cluster trust.

$$T1(S,D,\mathrm{Data}) = T(\mathrm{CD},D,\mathrm{Data}) \times \mathrm{CLT}(\mathrm{CS},\mathrm{CD}) \tag{11}$$

In Equation (11), *T*1 (*S*, *D*, Data) is the trust between trustor node *S* and *D* trustee in a way that *S* node existed in a cluster that CS node is its cluster head and *D* node existed in a cluster that CD node is its cluster head. *T* (CD < D, *D* Data) is Data authority over *D* node and calculated relating to CD cluster end node, also CLT (CS, CD) cluster authority, determines CS trustor cluster head for CD trustor cluster head.

Implementation and tests

In an analysis program, in this paper, we considered part of Epinions trust web network that consist of a graph with 700 nodes and 33,200 edges. We need trust value with real values for edges. In order to allocate values to the edges, we used Richardson Technique which created trust allocation in trust web network with normal distribution (Richardson et al., 2003). It is clear that if there is a link between two nodes, it shows that an interaction occurred in the past, so the trust deduced from trusty behaviours not from history chain. Only when there is no direct link between two nodes, it is necessary to perform trust estimation. In test, if there is a direct path between two nodes of trust web network, trust calculation is also performed in an indirect path. We compared two values and considered the greatest value as trust. In order to find network paths, Dijestra idea has been used to pass shorter paths earlier. We use different Metrics for evaluating accuracy in this study (Cormen, Leiserson, Rivest, & Stein, 2009).

Absolute error: indicated the difference between real value of trust for an edge and calculated value, by means of algorithm which is calculated by Equation (12).

$$\text{Absolute error } = |\text{calculated trust by means of an algorithm} - \text{real trust}| \tag{12}$$

In web trust network, the goal of calculating the value of trust is making a decision that if a trustor node could trust a trustee node or not. For example, if we obtain high trust value, we could trust the trustee otherwise, we decide not to trust. Based on application, we could consider a threshold as the ratio between trust and distrust. We consider this threshold as .5 in this study. If calculated value of trust was equal or more than .5, we could trust the trustee node; otherwise we could not trust the trustee node. We use precision and recall metrics for comparing methods accuracy. Precision and recall in three following conditions are as follows (Shekarpour & Katebi, 2010):

Trust conditions: in this condition, parameters used for accuracy calculation will be as follows (Equation (13)):

At: number of nodes which we trust them in real world.

Bt: number of nodes that the algorithm proposed to trust them.

$$\text{recall}_t = \frac{A_t \cap B_t}{A_t}, \ \text{precision}_t = \frac{A_t \cap B_t}{B_t} \tag{13}$$

Lack of trust conditions: in this condition, parameters used for calculating accuracy are as follows (Equation (14)):

Ad = number of nodes we do not trust them in the real world.

Bd = number of nodes that the algorithm proposed not to trust them.

$$\text{recall}_d = \frac{A_d \cap B_d}{A_d}, \ \text{precision}_d = \frac{A_d \cap B_d}{B_d} \tag{14}$$

General conditions: in this condition, parameters used for calculating accuracy are as follows (Equation (15)):

$$\text{recall} = \frac{(A_t \cap B_t) + (A_d \cap B_d)}{A_t + A_d}, \ \text{precision} = \frac{(A_t \cap B_t) + (A_d \cap B_d)}{B_t + B_d} \tag{15}$$

Anyway, there is a balance between precision and recall. For example, when the given value in set *A* is close to zero, recall value is near one, but precision value is near zero. We use Fscore criteria to measure recall and precision together (Equation (16)).

There are absolute errors and precision for continuous spectra and recall and Fscore for discrete cases.

$$\text{FScore} = \frac{2 \times \text{recall} \times \text{precision}}{\text{recall} + \text{precision}} \tag{16}$$

In this research, we used fuzzy clustering to select the cluster heads. In fuzzy clustering, every point has a degree of belonging to clusters, as in fuzzy logic, rather than belonging completely to just one cluster. Thus, points on the edge of a cluster may be in the cluster to a lesser degree than points in the centre of cluster. An overview and comparison of different fuzzy clustering algorithms is available (Nock & Nielsen, 2006). Any point *x* has a set of coefficients giving the degree of being in the *k*-th cluster $w_k(x)$. With fuzzy c-means, the centre of a cluster is the mean of all points, weighted by their degree of belonging to the cluster, according to Equation (17) is obtained.

$$C_k = \frac{\sum_x w_k(x)^m x}{\sum_x w_k(x)^m} \tag{17}$$

The degree of belonging, $w_k(x)$, is related inversely to the distance from *x* to the cluster centre as calculated on the previous pass. It also depends on a parameter *m* that controls how much weight is given to the closest centre. For example, in this research FCM algorithm as shown to classification of 700 nodes to 6 clusters in Figure 6.

For more details about the FCM algorithm, it consists of the following steps:

- Step 1: Let us suppose that M-dimensional *N* data points represented by *xi* ($i = 1, 2, \ldots, N$), are to be clustered.
- Step 2: Assume the number of clusters to be made, that is, *C*, where $2 \le C \le N$.
- Step 3: Choose an appropriate level of cluster fuzziness $f > 1$.
- Step 4: Initialise the $N \times C \times M$ sized membership matrix *U*, at random, such that $U_{ijm} \in [0, 1]$ and $\sum_{j=1}^{C} U_{ijm} = 1$, for each *i* and a fixed value of *m*.
- Step 5: Determine the cluster centres CC_{jm}, for *j*th cluster and its *m*th dimension using according to Equation (18).

$$\text{CC}_{jm} = \frac{\sum_{i=1}^{N} U_{ijm}^{f} x_{im}}{\sum_{i=1}^{N} U_{ijm}^{f}} \tag{18}$$

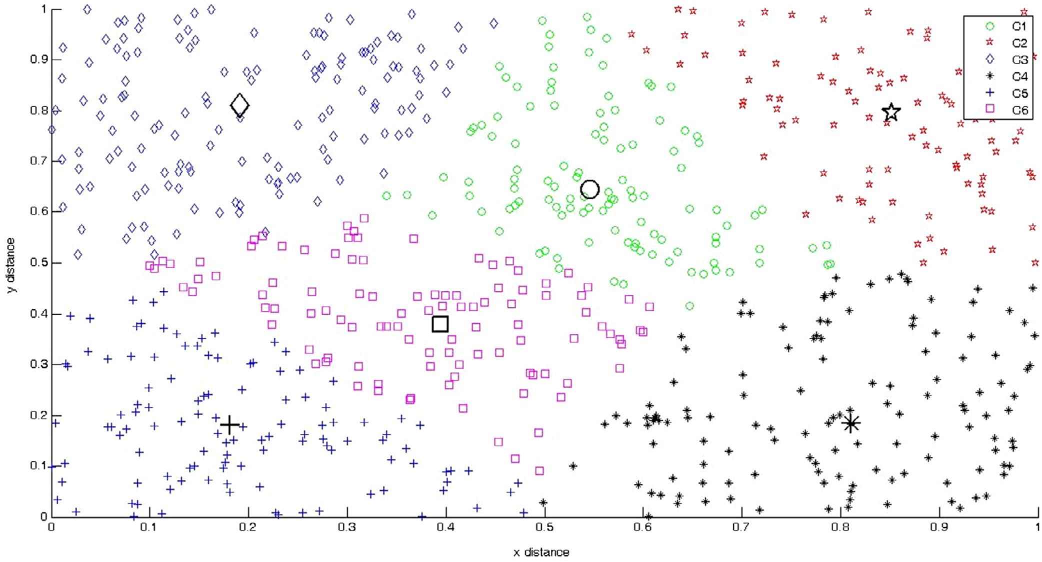

Figure 6. Classification of 700 nodes to 6 clusters.

- Step 6: Calculate the Euclidean distance between *i*th data point and *j*th cluster centre with respect to, say *m*th dimension like the Equation (19).

$$D_{ijm} = \left\| \left(x_{im} - CC_{jm} \right) \right\| \tag{19}$$

- Step 7: Update fuzzy membership matrix *U* according to D_{ijm}. If $D_{ijm} > 0$, Then If $D_{ijm} = 0$, then the data point coincides with the corresponding data point of *j*th cluster centre CC_{jm} and it has the full membership value, that is, $U_{ijm} = 1.0$ based on Equation (20).

$$U_{\text{ijm}} = \frac{1}{\sum_{c=1}^{C} \left(\frac{D_{ijm}}{D_{icm}} \right)^{\frac{2}{f-1}}} \tag{20}$$

- Step 8: Repeat from Step 5 to Step 7 until the changes in $U \leq \varrho$, where ϱ is a pre-specified termination criterion (Chattopadhyay, Pratihar, & De Sarkar, 2011).

In the proposed algorithm, in order to reach appropriate cluster numbers, at first we assume that parameters values of *α*, *β* and *γ* are equal and we test the number of clusters from 1 to 20 and Fscore value generally obtained for any of these modes. As we can see in Figure 7, if cluster numbers was 8, the greatest value of Fscore is obtained in general mode. Based on results, there is no direct logical relation between increasing cluster numbers and increasing trust; anyway, Fscore value will be greater in clustering model in comparison with centralised trust model.

In proposed algorithm three parameters *α*, *β* and *γ* are expressed which any of them in trust calculation determines the effect of social network trust parameters, trust of pages links values and semantic trust respectively. In order to obtain appropriate values for parameters *α*, *β* and *γ* in proposed algorithm, we calculate Fscore value in general mode with different values of parameters *α*, *β* and *γ* by considering 8 clusters. The result is shown in Figure 8. As we can see in Figure 8, the most appropriate Fscore value in general mode is as follows:

$\alpha = .3$, $\beta = .3$ and $\gamma = .4$.

We test Eigen trust algorithm (Kamvar et al., 2003), Tidal trust algorithm (Golbeck, 2006b) and proposed method over selected data from Epinions trust web network. In proposed method, number of

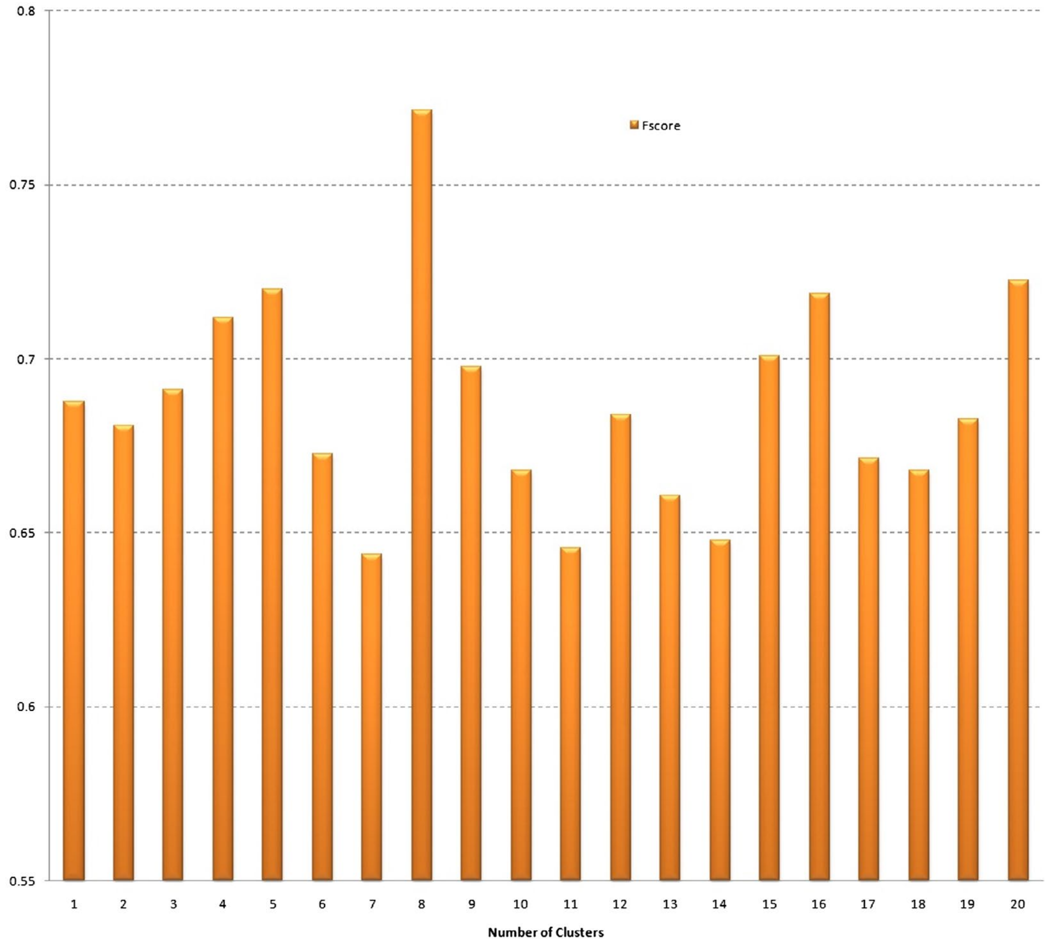

Figure 7. F score calculation of proposed algorithm in general mode for different cluster numbers.

clusters is 8 and parameters $\alpha = .3$, $\beta = .3$ and $\gamma = .4$. The evaluation of results accuracy is indicated in Tables 1–3.

Table 1 indicates the evaluation of accuracy results based on different metrics in trust state. The number of nodes which Eigen trust algorithm trusts them is more than the number of real trustee nodes, so that it has relatively low precision value but high recall value, Tidal trust algorithm usually trusts less nodes than real valid nodes so that it has relatively low recall value. But due to obtained valid nodes by this algorithm in many states will be the same as real valid nodes with high precision value. Proposed algorithm has more balanced results and has higher Fscore than two other methods in trust state.

Table 2 indicates the evaluation of results accuracy based on different metrics in distrust state. The number of nodes which Tidal trust algorithm does not trust them is more than the number of real distrust nodes, so that it has relatively low precision value but high recall value. The number of nodes which Eigen trust algorithm does not trust them is less than the number of real distrust nodes. So that it has relatively low recall value but due to distrust nodes obtained by this algorithm in most cases is equal to real distrust nodes, it has high precision value. Proposed algorithm has more balanced results and greater Fscore than two other methods in distrust mode.

Table 3 indicates the evaluation of results accuracy based on different metrics in general mode. As we consider that our proposed method in this paper has greatest Fscore and the least mean of error. In general, based on results, the proposed method has acceptable efficiency.

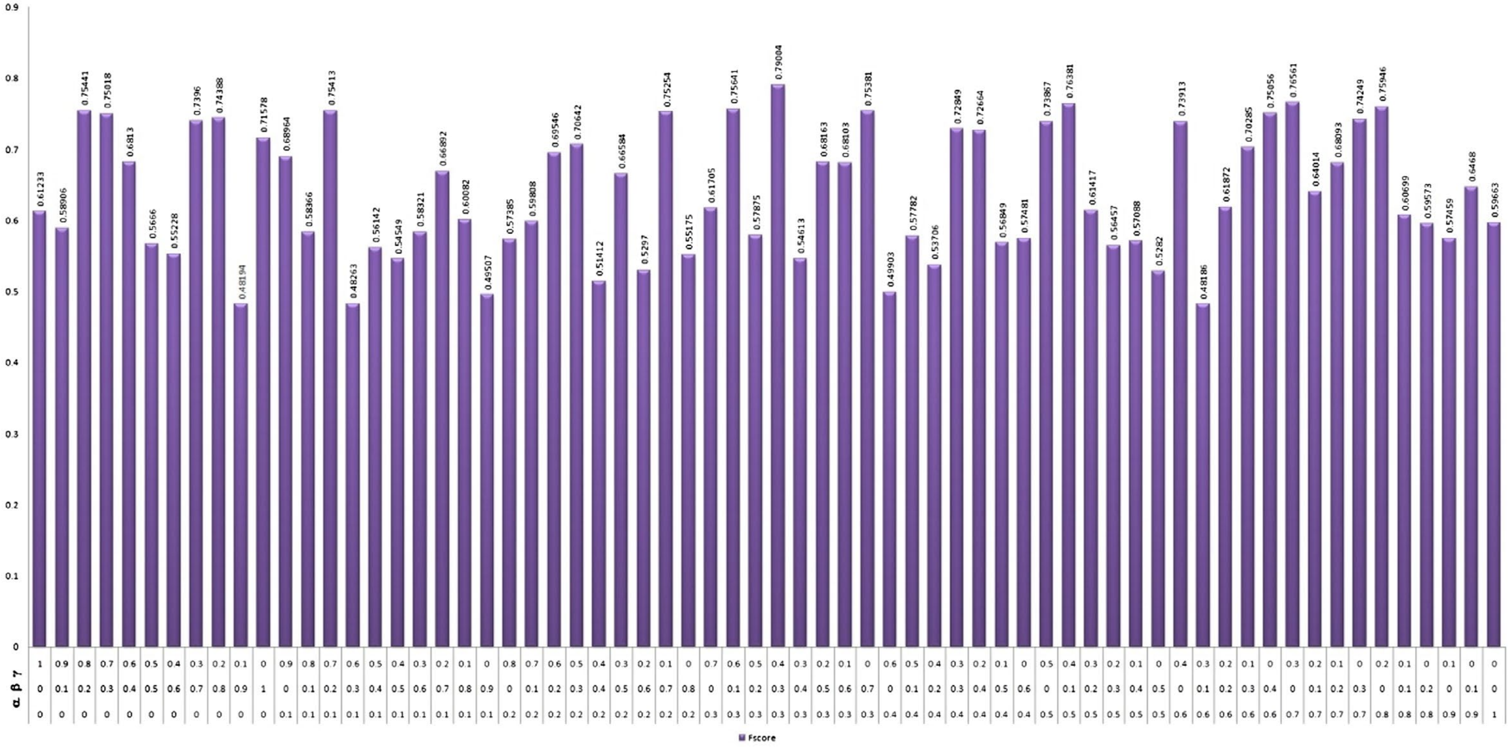

Figure 8. F score calculation of proposed algorithm in general mode for different values of α, β, γ.

Table 1. Results accuracy evaluation based on different metrics in trust mode.

	Metrics		
Algorithm	Recall	Precision	Fscore
Eigen trust	.83121	.51176	.63350
Tidal trust	.51911	.81095	.63301
Proposed algorithm	.76433	.79734	.78049

Table 2. Results accuracy evaluation based on different metrics in distrust mode.

	Metrics		
Algorithm	Recall	Precision	Fscore
Eigen trust	.68333	.69257	.68792
Tidal trust	.93333	.57143	.70886
Proposed algorithm	.78667	.81379	.80000

Table 3. Results accuracy evaluation based on different metrics in general mode.

	Metrics			
Algorithm	Mean of error	Recall	Precision	Fscore
Eigen trust	.23633	.75896	.57816	.65634
Tidal trust	.21314	.72150	.64110	.67893
Proposed algorithm	.12836	.77524	.80541	.79004

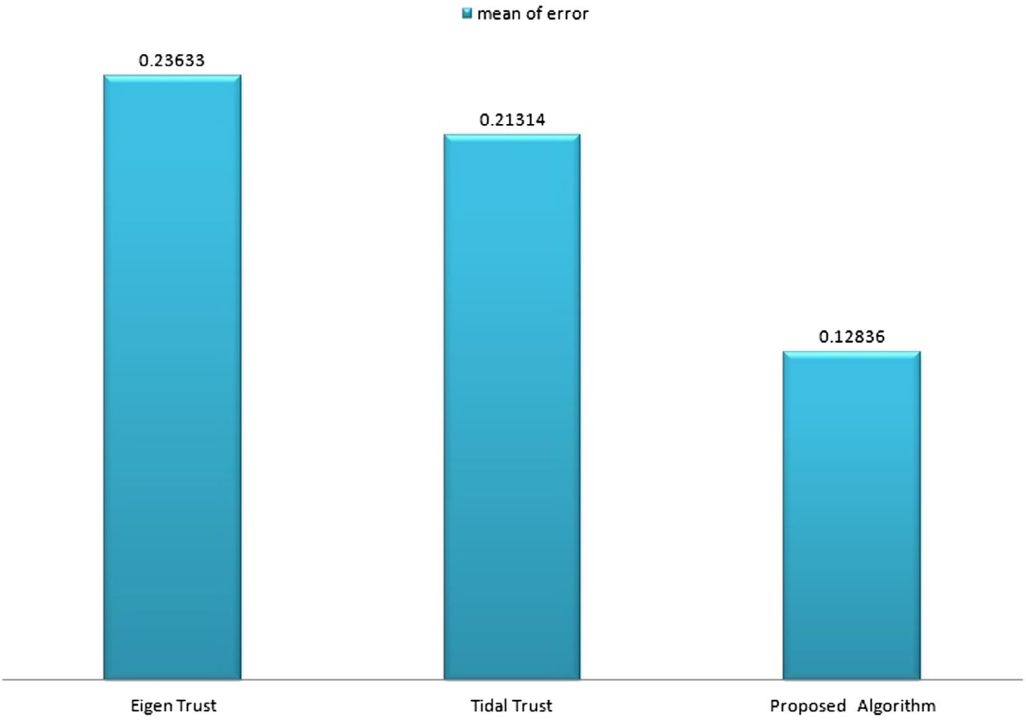

Figure 9. Mean of error for different methods.

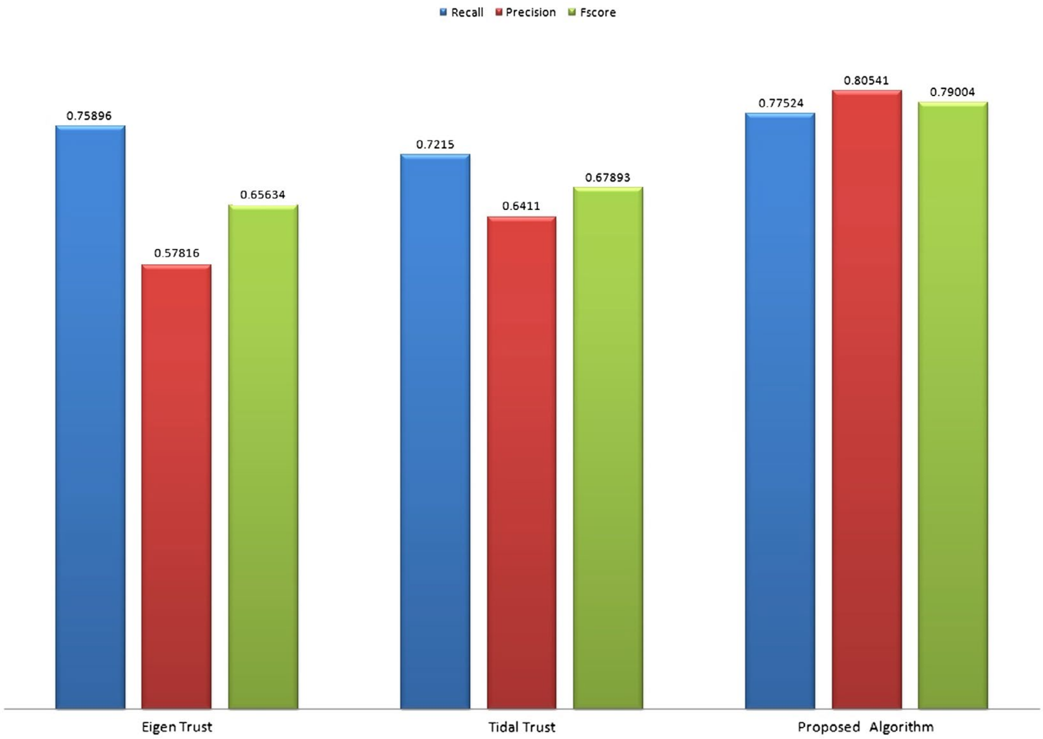

Figure 10. Recall, precision and Fscore parameters values for different methods in general mode.

Mean of error is shown for different methods in general mode in Figure 9, the proposed method's mean of error is 12.936% which is about 11% less than Eigen trust method and 8.5% less than Tidal trust method.

Figure 10 shows different parameters in general mode for various methods. The proposed method shows more than 79% Fscore that is about 13.5% more than Eigen trust method and about 11.5% more than Tidal trust method.

Clustering helps us to have small worlds of web of trust more specific. Often the nodes which locate in a cluster are dependent to each other and also they do their interactions with each other. This will help us to decrease the run time compared with global trust method with maintaining the accuracy of trust evaluation.

Conclusion

In this study different methods of trust estimation are investigated briefly. We used social network trust parameters, trust of pages links values and semantic trust in proposed algorithm to evaluate trust and based on performed tests, the effects of any of these parameters are considered .3, .3 and .4, respectively. Also we used clustering for increasing trust and scalability and we considered optimised number of cluster as 8 clusters. Based on results, the proposed method shows more than 79% Fscore that is about 13.5% more than Eigen trust method and about 11.5% more than Tidal trust method and 10.5% more than centralised trust method. Mean of error in this proposed method is 12.936 that is about 11% less than Eigen trust method and about 8.5% less than Tidal trust method. Finally, it could be said that proposed method presented has acceptable estimate for trust in web trust network. For proposing future works, we can use fuzzy systems instead of considering threshold limit for trust and distrust to decrease mean of error. Also, for performing a better clustering, clustering can be performed dynamically based on user semantic requests.

Acknowledgements

In performing our research, we had to take the help and guideline of some respected persons, who deserve our greatest gratitude. The completion of this research gives us much Pleasure. We would also like to expand our deepest gratitude to all those who have directly and indirectly guided us in writing this research.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by the Science and Research Branch, Islamic Azad University, Tehran, Iran.

References

Almendra, V. D. S., & Schwabe, D. (2006). Trust policies for semantic web repositories. In *Workshop at the 5th International Semantic Web Conference (ISWC)* (pp. 5–9), Athens.

Berners Lee, T., Handler, J., & Lassila, O. (2001, May). The semantic web. *Scientific American*, pp. 29–37.

Ceravolo, P., Damiani, E., & Viviani, M. (2005). Adding a peer-to-peer trust layer to metadata generators. In *OTM 2005 Workshops*, Cyprus (Lecture notes in computer science, vol. 3762, pp. 809–815).

Chattopadhyay, S., Pratihar, D. K., & De Sarkar, S. C. (2011). A comparative study of fuzzy C-means algorithm and entropy based fuzzy clustering algorithms. *Computing and Informatics, 30*, 701–720.

Chen, M., & Singh, J. P. (2001). Computing and using reputations for internet ratings. In *The 3rd ACM Conference on Electronic Commerce* (pp. 154–162), New York, NY, USA.

Chen, S., Wang, G., & Jia, W. (2015). K-fuzzy trust: Efficient trust computation for large-scale mobile social networks using a fuzzy implicit social graph. *Information Sciences, 318*, 123–143.

Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2009). *Introduction to algorithms* (3rd ed.). Cambridge: MIT Press and McGraw-Hill.

FOAF. (2000–2015). *An experimental linked information system*. Retrieved from http://www.foaf-project.org/

Golbeck, J. (2005). *Computing and applying trust in web-based social networks* (Ph.D. thesis). University of Maryland, College Park, MD, USA.

Golbeck, J. (2006a). Trust on the World Wide Web: A survey. *Foundations and Trends in Web Science, 1*, 131–197.

Golbeck, J. (2006b). Combining provenance with trust in social networks for semantic content filtering. In *Proceeding of the International Provenance and Annotation Workshop* (Lecture notes in computer science, vol. 4145, pp. 101–108), Chicago, IL, USA.

Golbeck, J., & Hendler, J. (2004). Accuracy of metrics for inferring trust and reputation in semantic web-based social networks. In *Proceedings of 14th International Conference on Knowledge Engineering and Knowledge Management* (Lecture notes in computer science, vol. 3257, pp. 116–131), October 5–8, Northamptonshire, UK.

Golbeck, J., Parsia, B., & Hendler, J. (2003). Trust network on the semantic web. In *Proceedings of Cooperative Information Agents VII* (Lecture notes in computer science, vol. 2782, pp. 238–249), August 27–29, Helsinki, Finland.

Guha, R., Kumar, R., Raghaven, P., & Tomkins, A. (2004). Propagation of trust and distrust. In *The 13th International Conference on World Wide Web* (pp. 403–412), ACM, New York, NY, USA.

Jamali, M., & Abolhassani, H. (2006). Different aspects of social network analysis. In *Proceedings of IEEE/WIC/ACM International Conference on The Web Intelligence (WI-06)* (pp. 66–72), December 18–22, Hong Kong.

Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an internet store. *Information Technology and Management, 1*, 45–71.

Kamvar, S. D., Schlosser, M. T., & Molina, H. G. (2003) The Eigen trust algorithm for reputation management in p2p networks. In *The 12th International World Wide Web Conference* (pp. 640–651), ACM, New York, NY, USA.

Kim, Y. A., & Phalak, R. (2012). A trust prediction framework in rating-based experience sharing social networks without a Web of Trust. *Information Sciences, 191*, 128–145.

Kleinberg, J. (1998). Authoritative sources in a hyperlinked environment. In *Proc. Ninth Ann. ACM-SIAM Symp. Discrete Algorithms*, New York: ACM Press, *Journal of the ACM, 46*, 668–677.

Lassila, O., & Swick, R. (1999, February 22). *Resource description framework (RDF) model and syntax specification*. In W3C Recommendation, World Wide Web Consortium.

Lesani, M., & Bagheri, S. (2006). Applying and inferring fuzzy trust in semantic web social networks. In *Canadian Semantic Web Working Symposium (CSWWS 2006)* (pp. 23–43), Quebec City, Canada.

Linn, J. Boeyen, S., Ellison, G., Karhuluoma, N., MacGregor, W., Madsen, P., … Thompson, P. (2004). *Trust models guidelines*. Retrieved from http://www.oasisopen.org/committees/documents.php?wgabbrev=security

Matsuo, Y., & Yamamoto, H. (2009). Community gravity: Measuring bidirectional effects by trust and rating on online social networks. In *Proceedings of the 18th International Conference on World Wide Web* (pp. 751–760), ACM, New York, NY, USA Madrid, Spain.

Milgram, S. (1967). The small world problem. *Psychology Today, 1*, 61–67.

Nock, R., & Nielsen, F. (2006). On weighting clustering. *IEEE Trans. on Pattern Analysis and Machine Intelligence, 28*, 1–13.

O'Donovan, J., & Smyth, B. (2006). Mining trust values from recommendation errors. *International Journal on Artificial Intelligence Tools, 15*, 945–962.

Page, L., Brin, S., Motwani, R., & Winograd, T. (1998). *The page rank citation ranking: Bringing order to the web* (pp. 1–17, Technical Report). Stanford University, San Francisco, Info Lab.

Pitsilis, G., & Chia, P.H. (2010). Does trust matter for user preferences? A study on Epinions ratings. In *The 4th IFIP International Conference on Trust Management (IFIPTM 2010)* (IFIP advances in information and communication technology, vol. 321, pp. 232–247), Morioka, Japan.

Richardson, M., Agrawal, R., & Domingos, P. (2003). Trust management for the semantic web. In *The 2nd International Semantic Web Conference* (Lecture notes in computer science Sanibel Island, vol. 2870, pp. 351–368.

Sabater, J., & Sierra, C. (2005). Review on computational trust and reputation models. *Artificial Intelligence Review, 24*, 33–60.

Shafiq, O., Alhajj, R., & Rokne, J. G. (2015). On personalizing Web search using social network analysis. *Information Sciences, 314*, 55–76.

Shekarpour, S., & Katebi, S. D. (2010). Modeling and evaluation of trust with an extension in semantic web. *Web Semantics: Science, Services and Agents on the World Wide Web, 8*, 26–36.

Tang, J., Gao, H., Liu, H., & Sarma, A. D. (2012). eTrust: Understanding trust evolution in an online world. In *The Eighteenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 253–261), ACM, New York, NY, USA.

Turel, O., Yuan, Y., & Connelly, C. E. (2008). In justice we trust: Predicting user acceptance of e-customer services. *Journal of Management Information Systems, 24*, 123–151.

Victor, P., Cornelis, C., Cock, M. D., & Teredesai, A. (2008). Key figure impact in trust-enhanced recommender systems. *AI Communications, 21*, 127–143.

W3School. (2010). *Semantic web tutorial*. Retrieved January 6, from http://www.w3schools.com/-semweb/default.asp

Yuan, W., Guan, D., Lee, Y. K., Lee, S., & Hur, S. J. (2010). Improved trust-aware recommender system using small-worldness of trust networks. *Knowledge-Based Systems, 23*, 232–238.

Ziegler, C. N., & Lausen, G. (2005). Propagation models for trust and distrust in social networks. *Information Systems Frontiers, 7*, 337–358.

Zolfaghar, K., & Aghaie, A. (2011). Evolution of trust networks in social web applications using supervised learning. *Procedia Computer Science, 3*, 833–839.