The ISC Int'l Journal of Information Security

ISeCure

July 2012, Volume 4, Number 2 (pp. 1–15)

http://www.isecure-journal.org

A Confidence-Aware Interval-based Trust Model

Hassan Shakeri [1,*] and Abbas Ghaemi Bafghi [1]

[1] *Department of Computer Engineering, Ferdowsi University of Mashhad, Mashhad, Iran*

ARTICLE INFO.

Article history:
Received: 21 January 2013
Revised: 04 March 2013
Accepted: 15 April 2013
Published Online: 4 August 2013

Keywords:
Trust, Confidence, Trust Interval, Trust Aggregation, Trust Propagation, Confidence Estimation.

ABSTRACT

It is a common and useful task in a web of trust to evaluate the trust value between two nodes using intermediate nodes. This is widely used when the source node has no experience of direct interaction with the target node or the direct trust is not reliable enough by itself. If trust is used to support decision-making, it is important to have not only an accurate estimate of trust, but also a measure of confidence in the intermediate nodes as well as the final estimated value of trust. The present paper thus aims to introduce a novel framework for integrated representation of trust and confidence using intervals which provides two operations of trust interval multiplication and summation. The former is used for computing propagated trust and confidence, whereas the latter provides a formula for aggregating different trust opinions. The properties of the two operations are investigated in details. This study also proposes a time-variant method that considers freshness, expertise level and two similarity measures in confidence estimation. The results indicate that this method is of more accuracy compared to the existing methods. In this regard, the results of experiments carried out on two well-known trust datasets are reported and analyzed, showing that the proposed method increases the accuracy of trust inference in comparison with the existing methods.

1 Introduction

Recently the concept of trust has been playing an increasingly important role in various fields of computing science including soft security, multi-agent systems, semantic web, computer networks, e-commerce, game theory, social networks, etc.

There exist a few definitions for trust in the literature, one of the most popular of which is the one proposed by Olmedilla *et al.* [3]: "Trust of a party A to a party B for a service X is the measurable belief of A in that B behaves dependably for a specified period within a specified context (in relation to service X)."

One may consider a *web of trust* in a society (of people or systems), i.e. a directed graph in which the vertexes denote the entities and the edge labels reflect the trust each entity maintains in every other entity.

If there is no link between a pair of entities in the web of trust, then no trust decision has yet been made. This is the case in which trust transitivity can be applied: if A trusts B and B trusts C, then A can trust C. This property is also known as trust propagation or indirect trust estimation. However there is an ongoing debate on how much transitivity to consider as valid and which formula or algorithm to use for evaluating propagated trust value in each field.

* Corresponding author.
Email addresses: shakeri@mshiau.ac.ir (H. Shakeri), ghaemib@um.ac.ir (A. Ghaemi Bafghi).
ISSN: 2008-2045

In this regard, multiple researchers are exploring ways to transfer trust within a web of trust. Examples of such efforts can be found in [4–6].

One of the major problems in indirect trust estimation based on the intermediate nodes is to ensure how reliable the result is when an intermediate node reports the value of trust it has in the target node. It is also difficult to determine how the level of confidence is to be applied in final trust estimation. Yet another relevant problem is to compute the resultant values of the trust in the target node, as reported independently by two or more intermediate nodes with known confidence levels, and also to estimate the confidence level of the reults. In other words, the following problems are to be dealt with:

- Representation of confidence
- Evaluation of each appraiser's confidence
- Confidence-aware trust propagation
- Confidence-aware trust aggregation

As an example, consider the web of trust in Figure 1 in which the source node, S, has two trust chains towards the destination (target) node, D. The label on the edge SA, for instance, shows that S's trust in A is 0.7; however there is only a confidence of 0.5 in this trust estimation. The other edge labels in the graph can be interpreted in a similar way. Now, in order to estimate the trustworthiness level of D, it is important to know how S is to apply the confidence labels in trust propagation in each chain, and consequently, how it should consider the confidence values to compute the resultant of trust values obtained from the two chains, and finally, how confident S's final judgment is.

Many of research studies, however, have not taken into account the role of confidence in trust management; and some of them including [7–9] have used the weighted-averaging method to consider the effect of the confidence in computing trust resultant. In this respecty, the present paper aims to introduce a novel idea to use the concept of interval for integrated representation of trust and confidence. Based on this representation, we propose a method, called trust interval multiplication, for propagating trust and confidence. We also present a method for aggregating two or more trust opinions, named as summation of trust intervals. The properties of the two operators are investigated. It is also shown that, in comparison with the existing methods, these operators are more accurate for evaluation of trust. In fact, the ideas of trust intervals and aggregating trust were driven by the ones proposed in [1] while the trust propagation method was proposed using trust intervals in [2]. Integrating these ideas, the present paper attempts to serve the following purposes: (a) proposing a new algorithm for confidence estimation based on the four measures of

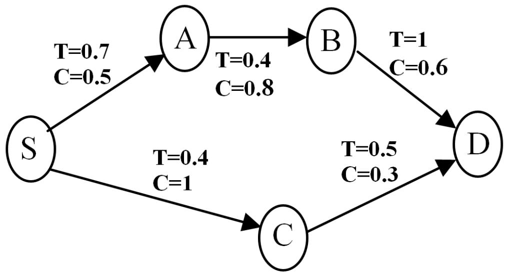

Figure 1. A sample web of trust including confidence values.

freshness, expertise level and two similarity measures, (b) conducting more formal analyses comparing to [1] and [2], (c) drawing comparisons between the proposed method and some existing well-known methods, and (d) addressing the problem of dependent paths in trust network.

To this end, the rest of this paper is organized as follows: Section 2 reveiws the related literature. In Section 3, a description of the interval representation of trust and confidence is put forth followed with the representation of operators on trust intervals. The properties of these operators are also investigated in this section. The proposed algorithm for inferring confidence-aware trust and the related formulas for confidence estimation are described in section Section 4. Section Section 5 deals with reporting and analysis of the results of the experiments carried out on two trust datasets using both the proposed algorithm and previous ones. Finally conclusions will be drawn in Section 6.

2 Related Work

Various research studies have been carried out in the area of trust transition and inferring.

Ding *et al.* in [10], for example, identified five types of trust, one of which, called STT, is used in the proposed algorithm. STT stands for Similar Trusting Trust and is an associative trust that evaluates the similarity of two agents' trust knowledge: STT_{ijd} refers to the similarity of agent ai and agent a_j's referral trust to the other agents within domain d.

Elsewhere, Golbeck in [6] proposed the well-known TidalTrust trust inference algorithm which is intended to be used for inferring trust in networks with continuous rating system. REGRET [11] first introduced by Sabater, is a decentralized trust model that uses witness agent recommendations as well as direct experiences of the source in trust estimation. Yet another well-known trust model is Travos [12] that takes into consideration the dynamicity of the agent behavior. Similarly, SUNNY [7] is a trust inference algorithm which uses a probabilistic sampling technique to estimate the confidence and computes the trust only based on information sources with high confidence estimates.

It is noteworthy that in some access control models, the propagated trust is evaluated using Iterative Multiplication Strategy, i.e. multiplying the labels of edges in the path from source to target in the web of trust [13, 14].

Yet there exist several studies dealing with confidence in trust management. Most of such projects, including [15–17], have considered the confidence as certainty which is described in [15] through the following example: Consider N white and black balls in a bin, knowing that at least m balls are white and n balls are black. Suppose p is the probability that a ball picked randomly from this bin, is white and c is the confidence in this probability. Since we have partial knowledge, we can estimate $p=m/N$ with $c=(m+n)/N$.

Some researches in the field have focused their attention to the parameters of confidence. In this regard, FIRE [9] is one of the most important trust models in this area as it takes into account several parameters, e.g. reliability of source and recency and relevance of ratings. In fact, this model incorporates interaction trust, role-based trust, witness reputation, and certified reputation to provide trust metrics. SecuredTrust [18] uses almost the same factors for estimating the confidence. FCTrust [19] is a distributed trust model based on feedback credibility (FC) which considers transaction density factor and similarity of ratings as the main parameters of confidence and then uses this confidence as the weight of ratings in aggregated trust estimation. CRM [20] is a trust framework which applies a number of measurements to evaluate the confidence, e.g. credibility of the contributing agents, the number of interactions, and timely relevance. In [21] a multi-attribute reputation management (MARM) support tool is proposed to assist users in choosing sellers in auction sites. This model estimates the confidence by combining four featured factors, i.e. similarity of the commodity category, value of each trade, time decay, and credibility of the feedback. In [7, 8] also, the value of confidence is estimated using similarity measures.

Some other studies have focused on a representation of confidence and/or approaches to propagation and aggregation of confidence-aware trust. One of the first works in this area is the one conducted by Jøsang and Knapsdog [16].They represent a trust opinion using a triple b, d, u in which b, d and u denote belief, disbelief and uncertainty respectively. They also introduce a subjective logic with operators for opinion propagation and aggregation as follows:

1) Let A and B be two agents so that $w_B^A = \{b_B^A, d_B^A, u_B^A\}$ is A's opinion about trustworthiness of B, and $w_C^B = \{b_C^B, d_C^B, u_C^B\}$ is B's opinion abou trustworthiness of C reported to A. Then A's opinion about trustworthiness of C based on the recommendation from B is defined by [16]:

$$w_C^{A:B} = w_B^A \otimes w_C^B = \{b_C^{A:B}, d_C^{A:B}, u_C^{A:B}\}, \quad (1)$$

where

$$\begin{cases} b_C^{A:B} = b_B^A b_C^B, \\ d_C^{A:B} = b_B^A d_C^B, \\ u_C^{A:B} = d_B^A + u_B^A + b_B^A u_C^B. \end{cases} \quad (2)$$

2) Let $w_C^A = \{b_C^A, d_C^A, u_C^A\}$ and $w_C^B = \{b_C^B, d_C^B, u_C^B\}$ be opinions about trustworthiness of the same entity C, held by agents A and B, respectively. Then the aggregated opinion is expressed by [16]:

$$w_C^{A,B} = w_C^A \oplus w_C^B = \{b_C^{A,B}, d_C^{A,B}, u_C^{A,B}\}, \quad (3)$$

where

$$\begin{cases} b_C^{A,B} = \dfrac{b_C^A u_C^B + b_C^B u_C^A}{u_C^A + u_C^B - u_C^A u_C^B}, \\ d_C^{A,B} = \dfrac{d_C^A u_C^B + d_C^B u_C^A}{u_C^A + u_C^B - u_C^A u_C^B}, \\ u_C^{A,B} = \dfrac{u_C^A u_C^B}{u_C^A + u_C^B - u_C^A u_C^B}. \end{cases} \quad (4)$$

In their later works, Jøsang *et al.* extended and improved their opinion model and subjective logic. One of the problems addressed in these studies is that subjective logic requires trust graphs to be expressed in a canonical form with no dependent paths. In the same vein, they proposed an approach to achieve independent trust edges based on edge splitting in [17].

Similarly, some researchers use Dempster-Shafer theory to deal with the issue of confidence in trust computing . For example in [22], trust opinions are represented as mass assignments in DST and then combined using Dempster's rule of combination to obtain the aggregated opinion.

Elsewhere in [23], four strategies for trust propagation and aggregation have been evaluated to maximize confidence in trust estimate. The strategies include weighted mean aggregation among shortest paths, min-max aggregation among shortest paths, weighted mean aggregation among all paths, and min-max aggregation among all paths

In [24], a model is proposed for aggregation of trust evidences which computes confidence scores taking into account the dynamic properties of trust.

To address the issue of unfair testimonies, a credibility model has been introduced in [25] which helps the trusters evaluate the confidence of the witnesses who provide testimonies on the trustees and guides the trusters how to filter and aggregate testimonies based on the evaluation of confidence.

In [26] the authors maintain that a single trust value cannot depict the real trust level very well under certain circumstances. They therefore suggest a trust vector which consists of three values: final trust level, service trust trend, and service performance consistency level. In fact, the two latter values represent some kind of confidence. The present paper also introduces an aggregation method in which each rating with a clear distance to the average of ratings is taken as marginal. Marginal ratings are then discarded in aggregation as they are not confident.

Most of the other studies in this regard, including [7–9], make use of the well-known weighted-averaging method to compute the resultant of trust opinions. In this method, when the source entity receives reports from two or more appraisers on the target entityŠs trustworthiness level, it considers its own confidence in each appraiser as the weight of that appraiser and then calculates the weighted average of all received values.

3 The Proposed Framework

In the field of trust management, confidence is considered as a metric that represents the accuracy of the trust values [27]. In fact, it denotes the capacity in which an entity is assured about its own or another entity's assessment on a target entity's trustworthiness level. In other words, the confidence that n has in n_0 is n's belief on the correctness of information provided by n_0 [7].

As an example, suppose that entity S asks entity A about D's trustworthiness level and A replies with 0.7. In this opinion, however, S's (or A's itself) confidence may be 0.8.

Therefore, there appears to exist a need to a suitable way of representing the concept of confidence along with trust. It is also important to have methods for propagating and aggregating confidence-aware trust opinions.

In this section, using intervals, we first introduce a novel idea of representing trust and confidence, both together. Then the two operations, multiplication and summation are defined on these intervals, which may be used for propagation and aggregation purposes.

3.1 Representation of Trust and Confidence using Interval Notation

When trust and confidence are denoted with two distinct numbers, simultaneous calculation of the two will be difficult. To bridge this gap, these two values are proposed to be integrated in a new representation using intervals, as shown in (5) below.

$$TI = [C * T, C * T + 1 - C] \tag{5}$$

Where TI is Trust Interval, and C and T are confidence and trust values respectively.

We now explain how the lower and upper bounds of the trust interval in (5) are obtained: in order to determine the lower bound of the trust interval, we should consider the case when base rate is $a = 0$. Base rate determines how uncertainty is to contribute to the opinion's probability expectation value [17]. C is the level of confidence and thus $1 - C$ is the value of uncertainty. Since trust is reported as T, the minimum value of the confident trust is $C * T$. Consequently, the lower bound of the trust interval is achieved as shown by (6).

$$L = C*T+(1-C)*a = C*T+(1-C)*0 = C*T. \tag{6}$$

To determine the upper bound of the trust interval, on the other hand, we should consider the case when a=1, finally arriving at [7] as for the upper bound.

$$\begin{aligned} U &= C * T + (1 - C) * a \\ &= C * T + (1 - C) * 1 \\ &= C * T + 1 - C. \end{aligned} \tag{7}$$

As an example, assume $T = 0.7$. With some different values of C, the trust intervals will be as follows:

$$C = 0 \rightarrow TI = [0, 1]$$

$$C = 0.5 \rightarrow TI = [0.35, 0.85]$$

$$C = 0.8 \rightarrow TI = [0.56, 0.76]$$

$$C = 1 \rightarrow TI = [0.7, 0.7]$$

In fact, in the case of $C = 0$, there is no confidence in the opinion of the appraiser at all. This means that no valuable knowledge is obtained about the trustworthiness level of the target. Therefore, the trust interval is [0,1]. Note that in the case of $C = 0$, the trust interval is independent of the value of T and is always [0,1]. As C is increased, the trust interval becomes narrower and the lower and upper bounds approach to T. Finally in the case of $C = 1$, there is an absolute confidence in the appraiser's opinion. Hence, the trust estimation is quite accurate and the lower and upper bounds of the trust interval are the same and equal to T, i.e. [0.7,0.7], in our example.

It is believed that using an integrated interval for representing both trust and confidence is clearer and more intuitive in comparison to using two distinct variables for them. However, the values of trust and confidence can be again extracted from the trust interval anytime needed, especially for evaluation purposes where different methods are to be compared. To this end, one may consider (6) and (7) as a system of two equations and solve the system for T and C. Thus, trust and confidence will be obtained as in (8) and (9).

$$T = \frac{L}{1+L-U} = \frac{L}{1-W} \tag{8}$$

$$C = 1 - W \tag{9}$$

where W is the width of the trust interval, defined as

$$W = U - L \tag{10}$$

The idea of using interval concept for representing trust and confidence proposed here is conceptually similar to the one introduced by Jøsnag in [16]. As mentioned earlier in Section 2, Jøsnag's model uses a triple to represent belief, disbelief, and uncertainty. However, it is believed that, due to using the well-known concept of interval, the proposed notation is more intuitive compared with the one put forth by Jøsang. It has to be noticed yet, that these two notations are convertible to each other. For instance, using (11) and (12), we can easily convert Jøsang's notation to our proposed model.

$$L = B \tag{11}$$

$$U = 1 - d \tag{12}$$

Note that in Jøsang's notation, u is not an independent variable and may be obtained having b and d as $u = 1 - (b + d)$. The value of u is equivalent to the width of the trust interval in our representation. For example, the triple 0.5,0.3,0.2 in Jøsang's model is represented as the interval [0.5,0.7] in the new notation.

The center of a trust interval may be considered as the probability expectation value of trust, when $a = 0.5$. It should not be mistaken for the value of T that is obtained from (8). Consider the trust interval [0.6,0.8] for example. The center of the interval is 0.7 meaning that, supposing $a = 0.5$, the expectation value of trust is 0.7. The value of 0.75, on the other hand, is obtained for T from (8), with a value of 0.8 for C obtained from (9). From the probability point of view, we may arrive at the conclusion that "with the probability of 0.8, the trust value is 0.75, while with the probability of 0.2 the trust value is unknow". As another example, consider the trust interval [0.4,1]. The center of this interval is also 0.7. Therefore, once again the expectation value of trust, for $a = 0.5$, is 0.7. However, the values of 1 and 0.4 are obtained from (8) and (9) for T and C, respectively. In fact, though the expectation values of trust in the two intervals are the same, the first interval reflects a higher level of confidence.

3.2 Trust Interval Multiplication

Suppose that the entity S (source) has some trust in the intermediate entity X represented by $[L_{SX}, U_{SX}]$. S asks X to report its opinion about the trustworthiness level of the entity D (destination or target). X replies in the form of trust interval $[L_{XD}, U_{XD}]$ (In practice S may first receive from X the values of trust and confidence as distinct variables. In such a case it should calculate the trust interval using (5), replacing T in (5) with X's reported trust in D, and C with X's confidence in its own opinion). To determine the final assessment of S on D's trustworthiness as the value of propagated trust, and the capacity in which this estimation is confident, a special kind of multiplication operator is being defined for trust intervals, as represented in (13)-(15). Note that this does not refer to the classic interval multiplication operator, but rather a novel operator which reflects trust and confidence propagation.

$$[L_{SX}, U_{SX}] \otimes [L_{XD}, U_{XD}] = [L_{SD}, U_{SD}] \tag{13}$$

such that

$$L_{SD} = L_{SX} L_{XD} \tag{14}$$

$$L_{SD} = 1 - L_{SX}(1 - U_{XD}) \tag{15}$$

Where $[L_{SD}, U_{SD}]$ denotes the final propagated trust interval.

Equations (14) and (15) are obtained from transferring (2) into interval space.

In order to illustrate the concept and applications of interval notation as well as the multiplication operator defined in (14) and (15), the product of some different pairs of intervals have been computed, the results of which are reported in Table 1. As expressed by (13), in interval multiplication, the upper bound of first interval is of no role. That is why it is denoted by x in the table.

Using (13)-(15) and the results summarized in Table 1, we now investigate some of the trust interval multiplication properties as described below:

1) If $[L_{SX}, U_{SX}] = [1, 1]$, then the product is equal to $[L_{XD}, L_{XD}]$. In other words, [1,1] is the left identity element for trust interval multiplication operator. This is justifiable because S has absolute confident trust in X and thus accepts its recommendations exactly.

2) The proposed operation of trust interval multiplication is not commutative. For example we have

$$[0, 0.33] \otimes [0.33, 0.66] = [0, 1],$$

whereas

$$[0.33, 0.66] \otimes [0, 0.33] = [0, 0.78].$$

3) The product is independent of U_{SX}. In other words, in trust interval multiplication, only the lower bound of the left operand is important. This is notcomes as no surpriseing because since in computing both the upper and lower bounds of the result interval, we should apply only the minimum of confident trust is to be applied from source to the intermediate node, i.e. L_{SX}. This is eEquivalent to the fact that in (2), d_{AB} has no role in computing $b_C^{A:B}$, $d_C^{A:B}$ and even $u_C^{A:B}$ (if we extend the formula of $u_C^{A:B}$, we see that it is independent of d_{AB}).

4) If $L_{SX} = 0$, then the product of two intervals will always be [0,1]. In fact, in such a case the source(S) has no confident trust in the intermediate node(X) at all; hence, X's recommendations do not provide any confident information to S. As mentioned before in this section, this case is represented by the trust interval [0,1].

5) If $[L_{XD}, U_{XD}] = [0, 1]$, then the product of trust intervals will also be [0,1]. This is true as in such a case, X has no confidence in its own assessment about D at all, and it is obvious that the propagated trust interval will be absolutely unconfident as well. It has to be noted again that the trust interval [0,1] reflects *zero confidence.*

6) Theorem 1 states that, in trust interval multiplication, the trust value of the result is equal to the trust value of the right operand.

Theorem 1. *Let's represent the values of trust related to the trust intervals* $[L_{XD}, U_{XD}]$ *and* $[L_{SD}, U_{SD}]$ *in* (13) *with* $[T_{XD}]$ *and* $[T_{SD}]$*, respectively. Then we will have* $[T_{SD} = T_{XD}]$.

Proof. Using (8), (14) and (15), we may write:

$$\begin{aligned} T_{SD} &= \frac{L_{SD}}{1 + L_{SD} - U_{SD}} \\ &= \frac{L_{SX} L_{XD}}{1 + L_{SX} L_{XD} - 1 + L_{SX}(1 - U_{XD})} \\ &= \frac{L_{XD}}{L_{XD} + (1 - U_{XD})} = \frac{L_{XD}}{1 + L_{XD} - U_{XD}} = T_{XD} \end{aligned}$$

□

3.3 Trust Interval Summation

Suppose that the entity S (source) asks two intermediate entities A and B to report their opinions about the trustworthiness level of the entity D (destination or target). A and B send their replies in the form of trust intervals $[L_A, U_A]$ and $[L_B, U_B]$, respectively. As mentioned above, it is possible for S to first receive the values of trust and confidence from A and B as distinct variables. In such a case it should calculate the trust interval using (5). For example, for calculating $[L_A, U_A]$, C in (5) should be replaced with S's confidence in A's opinion and T with A's reported trust in D. To determine what the final assessment of S is on D's trustworthiness as the resultant of A's and B's opinions, and in what capacity this estimation is confident, a special kind of summation operator for trust intervals is proposed, as illustrated in (16)-(17). Note again that this is not the classic interval summation operator, but a novel operator that determines the resultant of two opinions on the trustworthiness of a target entity.

$$[L_A, U_A] \oplus [L_B, U_B] = [L_C, U_C] \tag{16}$$

$$L_C = \frac{L_A U_B + L_B U_A - 2 L_A L_B}{W_A + W_B - W_A W_B}, \tag{17}$$

$$U_C = \frac{U_A U_B - L_A L_B}{W_A + W_B - W_A W_B}, \tag{18}$$

Where L_C and U_C denote the lower and upper bounds of the resultant's trust interval, respectively and W is the interval width.

Equations (17) and (18) are obtained from transferring (4) into the interval space.

In order to illustrate the summation operator defined in (16)-(18), we have computed the sum of some

Table 1. Product of some trust interval pairs.

Intervals	[0,0]	[0,0.33]	[0,0.66]	[0,1]	[0.33,0.33]	[0.33,0.66]	[0.33,1]	[0.66,0.66]	[0.66,1]	[1,1]
$[0, x], 0 \leq x \leq 1$	[0,1]	[0,1]	[0,1]	[0,1]	[0,1]	[0,1]	[0,1]	[0,1]	[0,1]	[0,1]
$[0.33, x], 0.33 \leq x \leq 1$	[0,0.67]	[0,0.78]	[0,0.89]	[0,1]	[0.11,0.78]	[0.11,0.89]	[0.11,1]	[0.22,0.89]	[0.22,1]	[0.33,1]
$[0.66, x], 0.66 \leq x \leq 1$	[0,0.34]	[0,0.56]	[0,0.78]	[0,1]	[0.22,0.56]	[0.22,0.78]	[0.22,1]	[0.44,0.78]	[0.44,1]	[0.66,1]
$[1, 1]$	[0,0]	[0,0.33]	[0,0.66]	[0,1]	[0.33,0.33]	[0.33,0.66]	[0.33,1]	[0.66,0.66]	[0.66,1]	[1,1]

Table 2. Sum (resultant) of some trust interval pairs.

Intervals	**[0,0.25]**	**[0,0.5]**	**[0,0.75]**	**[0,1]**	**[0.25,0.5]**	**[0.25,0.75]**	**[0.25,1]**	**[0.5,0.75]**	**[0.5,1]**	**[0.75,1]**
[0,0.25]	[0,0.14]	[0,0.2]	[0,0.23]	[0,0.25]	[0.14,0.29]	[0.1,0.3]	[0.08,0.31]	[0.29,0.43]	[0.2,0.4]	[0.43,0.57]
[0,0.5]	[0,0.2]	[0,0.33]	[0,0.43]	[0,0.5]	[0.2,0.4]	[0.17,0.5]	[0.14,0.57]	[0.4,0.6]	[0.33,0.67]	[0.6,0.8]
[0,0.75]	[0,0.23]	[0,0.43]	[0,0.6]	[0,0.75]	[0.23,0.46]	[0.21,0.64]	[0.2,0.8]	[0.46,0.69]	[0.43,0.86]	[0.69,0.92]
[0,1]	[0,0.25]	[0,0.5]	[0,0.75]	[0,1]	[0.25,0.0.5]	[0.25,0.75]	[0.25,1]	[0.5,0.75]	[0.5,1]	[0.75,1]
[0.25,0.5]	[0.14,0.29]	[0.2,0.4]	[0.23,0.46]	[0.25,0.0.5]	[0.29,0.43]	[0.3,0.5]	[0.31,0.54]	[0.43,0.57]	[0.4,0.6]	[0.57,0.71]
[0.25,0.75]	[0.1,0.3]	[0.17,0.5]	[0.21,0.64]	[0.25,0.75]	[0.3,0.5]	[0.33,0.67]	[0.36,0.79]	[0.5,0.7]	[0.5,0.83]	[0.7,0.9]
[0.25,1]	[0.08,0.31]	[0.14,0.57]	[0.2,0.8]	[0.25,1]	[0.31,0.54]	[0.36,0.79]	[0.4,1]	[0.54,0.77]	[0.57,1]	[0.77,1]
[0.5,0.75]	[0.29,0.43]	[0.4,0.6]	[0.46,0.69]	[0.5,0.75]	[0.43,0.57]	[0.5,0.7]	[0.54,0.77]	[0.57,0.71]	[0.6,0.8]	[0.71,0.86]
[0.5,1]	[0.2,0.4]	[0.33,0.67]	[0.43,0.86]	[0.5,1]	[0.4,0.6]	[0.5,0.83]	[0.57,1]	[0.6,0.8]	[0.67,1]	[0.8,1]
[0.75,1]	[0.43,0.57]	[0.6,0.8]	[0.69,0.92]	[0.75,1]	[0.57,0.71]	[0.7,0.9]	[0.77,1]	[0.71,0.86]	[0.8,1]	[0.86,1]

different pairs of trust intervals. Table 2 below summarizes the results in this regard.

Having (16)-(18) and the results in Table 2 at hand, we investigate some of the trust interval summation properties and explain in the following section how it gives the resultant of two or more opinions in different cases:

1) Sum of two similar or equal trust intervals reflects the confidence increment as the opinions confirm each other. For example sum of the two equal trust intervals [0.25,0.5] and [0.25,0.5] is [0.29,0.43]. As mentioned earlier, a reduction in the interval width indicates the increment of confidence.

2) If we add two or more different (and possibly contradictory) opinions, again the result interval will be narrower than both operand intervals. However, the result is a trust interval that reflects the resultant. Therefore, sum of the two intervals of [0,0.5] and [0.75,1], for instance, would be [0.6,0.8].

As another example, suppose that we are to determine the sum (resultant) of four people's opinions given in the form of trust intervals as follows:

$$P1 = [0.6, 0.8]$$
$$P2 = [0.6, 0.8]$$
$$P3 = [0.5, 0.75]$$
$$P4 = [0.1,\ 0.3]$$

The step-by-step calculation displays how the resultant is obtained for the first three opinions confirming each other and the fourth opinion contradicting them:

$$P_1 \oplus P_2 = [0.67, 0.78]$$
$$(P_1 \oplus P_2) \oplus P_3 = [0.67, 0.75]$$
$$((P_1 \oplus P_2) \oplus P_3) \oplus P_4 = [0.53, 59]$$

The resultant achieved in this way is different from the usual weighted average described in Section 2. In fact, this method for calculating the resultant is more accurate than the weighted average. Later in Section 5, we report the results of experiments confirming this idea.

3) The sum of any trust interval X and the interval [0,1] is X itself. In other words, [0,1] is the additive identity of the trust intervals. This property is explained here: as was discussed before, the trust interval [0,1] provides no valuable knowledge about the trustworthiness level of the target. Therefore, adding it to any other trust interval X has no affect and the sum will be X itself.

4) Theorem 2 states that in trust interval summation, the width of the result is always less than, or equal to, the width of each summed interval.

Theorem 2. *Let R be the resultant (sum) of two trust intervals A and B according to* (16)-(18) *and widths of the three intervals equal to W_R, W_A, and W_B respectively. Then we always have*

$$(a)\ \ W_R \leq W_A, \tag{19}$$

$$(b)\ \ W_R \leq W_B, \tag{20}$$

with equality possible only in the case where an arbitrary interval is summed to the interval [0,1].

Proof. (a) is proved below. The same procedure can be followed for (b) as well.

$$\begin{aligned} W_R = U_R - L_R &= \frac{U_A U_B + L_A L_B - L_A U_B - L_B U_A}{W_A + W_B - W_A W_B} \\ &= \frac{(U_A - L_A)(U_B - L_B)}{W_A + W_B - W_A W_B} \\ &= \frac{W_A W_B}{W_A + W_B - W_A W_B} \end{aligned} \tag{21}$$

$$W_R - W_A = \frac{W_A W_B}{W_A + W_B - W_A W_B} - W_A$$
$$= \frac{{W_A}^2 (W_B - 1)}{W_A + W_B - W_A W_B} \tag{22}$$

We know that $W_A^2 \geq 0$. On the other hand, WB is less than or equal to 1. Therefore, $W_B - 1 \leq 0$. In addition, since W_A and W_B are both less than or equal to 1, the denominator is a positive number. Then we have

$$W_R - W_A \leq 0$$

or

$$W_R \leq W_A$$

The fact that the width of sum interval is less than the width of each summed interval indicates that summation of two trust intervals magnifies the confidence and reduces the uncertainty. In fact, when the opinions of two people are being obtained, we have more confidence and less uncertainty comparing to the case where only the opinion of a single person is available. Obviously, the more numbers of opinions we add, the higher the confidence will be. In order to attain the maximum confidence, i.e. 1, infinite numbers of opinions need to be added.

□

5) Theorem 3 states that if two trust intervals with equal values of trust (T) are added, the trust value itself does not change.

Theorem 3. *Let R be the resultant (sum) of two trust intervals A and B that are based on the same value of trust, i.e. $T_A = T_B = T$, or equivalently*

$$\frac{L_A}{1 - W_A} = \frac{L_B}{1 - W_B} = T \tag{23}$$

then we will have

$$T_R = T \tag{24}$$

Proof. From (8), we have

$$T_R = \frac{L_R}{1 - W_R} \tag{25}$$

On the other hand, we may rewrite the formula for LR based on (17) as follows:

$$L_R = \frac{L_A U_B + L_B U_A - 2 L_A L_B}{W_A + W_B - W_A W_B}$$
$$= \frac{L_A (U_B - L_B) + L_B (U_A - L_A)}{W_A + W_B - W_A W_B}$$
$$= \frac{L_A W_B + L_B W_A}{W_A + W_B - W_A W_B} \tag{26}$$

Replacing the values of L_R from (26) and W_R from (21) in (25), we obtain

$$T_R = \frac{L_A W_B + L_B W_A}{W_A + W_B - 2 W_A W_B}$$
$$= \frac{L_A W_B + L_B W_A}{W_A (1 - W_B) + W_B (1 - W_A)}$$
$$= \frac{L_A \left(W_B + W_A \frac{L_B}{L_A} \right)}{(1 - W_A) \left(W_B + W_A \frac{1 - W_B}{1 - W_A} \right)} \tag{27}$$

From (23), we conclude

$$\frac{1 - W_B}{1 - W_A} = \frac{L_B}{L_A} \tag{28}$$

Merging (27) and (28), we arrive at

$$T_R = \frac{L_A (W_B + W_A \frac{L_B}{L_A})}{(1 - W_A) (W_B + W_A \frac{L_B}{L_A})} = \frac{L_A}{1 - W_A} = T \tag{29}$$

□

6) The proposed operation of trust interval summation is commutative. This property is obvious from (16)-(18). This property may also be observed in Table 2, which is symmetric with respect to the main diagonal.

7) The operator is associative as well. The proof for associativity, on the other hand, is simple, but too long to be included here. It can be illustrated using an example:

$$([0.2, 0.6] \oplus [0.35, 0.5]) \oplus [0.25, 0.8]$$
$$= [0.35, 0.47] \oplus [0.25, 0.8] = [0.37, 0.48]$$
$$[0.2, 0.6] \oplus ([0.35, 0.5] \oplus [0.25, 0.8])$$
$$= [0.2, 0.6] \oplus [0.37, 0.51] = [0.37, 0.48]$$

8) The commutativity and associativity properties imply that changing the order of the received opinions and summation process does not change the final result. One may argue that this is not true when people are to decide based on two or more recommendations. For example, one might not come up with the same conclusion if s/he receives a confirming opinion about something first and a disconfirming one later compared to when he receives the same two opinions in the reverse order. This can be accounted for by the subjectivity in human decision making. However, objective methods are to be employed in trust management as they will be executed by machines, even if the raw opinions are provided by people.

3.4 Scalar by Interval Multiplication

The width of the result interval comes even narrower, if more than two equal opinions are added. According to theorems 2 and 3, more equal opinions added together, yield more confidence in the resultant, without changing the trust. The sum of multiple equal opinions may be regarded as a kind of scalar by trust interval multiplication. Based on this, the results of multiplication of numbers 1 through 4 and also 100 by the trust interval [0.25,0.5] are presented in Table 3. It is to be noted again that this is not the classic scalar by interval multiplication, but a novel multiplication operator which describes the resultant of some equal opinions. The formal definition of this operator is as follows:

Definition 1. Let n is be a natural number, i.e. $n \in N_0$, and $[L, U]$ is be a trust interval. Then the scalar multiplication of n by $[L, U]$ is defined as:

$$n * [L, U] = \left[L^{(n)}, U^{(n)}\right]$$
$$= \begin{cases} [0,1], & n = 0 \\ [L, U] \oplus ((n-1) * [L, U]), & otherwise \end{cases}$$

Theorem 4 suggests formulas for calculating the result of scalar multiplication of trust intervals.

Theorem 4. *Let $[L^{(n)}, U^{(n)}]$ be the result of $n * [L, U], n \in N_0$, where the width of $[L, U]$ is W. Then we have*

$$L^{(n)} = \frac{nL}{n - (n-1) W} \tag{30}$$

$$U^{(n)} = \frac{U + (n-1) L}{n - (n-1) W} \tag{31}$$

Proof. Theorem can be proved using mathematical induction on n. However, the proof is, though rather simple, too long to be included here. □

Table 3. Summation of some equal opinions (Multiples of [0.25, 0.5]).

1*[0.25,0.5]	2*[0.25,0.5]	3*[0.25,0.5]	4*[0.25,0.5]	100*[0.25,0.5]
[0.25,0.5]	[0.29,0.43]	[0.3,0.4]	[0.31,0.38]	[0.33,0.34]

Theorem 5 determines the limit of $n * [L, U]$ when n approaches infinity.

Theorem 5. *Let T be the trust value on which the trust interval $[L, U]$ is constructed. Then*

$$\lim_{n\to\infty} [L^{(n)}, U^{(n)}] = [T, T] \tag{32}$$

Proof. According to (30), we have

$$\lim_{n\to\infty} L^{(n)} = \lim_{n\to\infty} \frac{nL}{n - (n-1) W}$$
$$= \lim_{n\to\infty} \frac{nL}{n\left(1 - \frac{n-1}{n} W\right)} \tag{33}$$

And we know

$$\lim_{n\to\infty} \frac{n-1}{n} = 1, \tag{34}$$

thus we will arrive at

$$\lim_{n\to\infty} L^{(n)} = \lim_{n\to\infty} \frac{nL}{n(1-W)} = \frac{L}{1-W} = T. \tag{35}$$

Similarly , from (31), we conclude

$$\lim_{n\to\infty} U^{(n)} = \lim_{n\to\infty} \frac{U + (n-1) L}{n - (n-1) W}$$
$$= \lim_{n\to\infty} \frac{n\left(\frac{U}{n} + \frac{n-1}{n} L\right)}{n\left(1 - \frac{n-1}{n} W\right)} \tag{36}$$

We also know that

$$\lim_{n\to\infty} \frac{U}{n} = 0 \tag{37}$$

Considering (34) and (37), we obtain from (36),

$$\lim_{n\to\infty} U^{(n)} = \frac{L}{1-W} = T \tag{38}$$

Now, the last column of Table 3 can be interpreted based on Theorem 5. □

3.5 Trust Intervals as an Algebraic System

Consider the set of all intervals in the range of 0 through 1, with distinct lower and upper bounds:

$$A = [a, b] | a, b \in [0, 1], a \neq b \tag{39}$$

The set A with our summation operator defined in (16)-(18) may be considered as an algebraic structure. This structure has two properties: associativity and identity element, which are investigated earlier in this section.Thus A may beconsidered as a *monoid*.

However, A is not a group, as it does not satisfy the invertibility property. To satisfy this property, for any interval, we would have $[a, b] \in A$, as well as an inverse interval [a’,b’] such that

$$[a, b] \oplus [a', b'] = [0, 1] \tag{40}$$

Nevertheless, this is impossible if the width of the interval [a,b] is less than 1, since, according to Theorem 2, the width of the result is always less than the width of each summed interval in such cases.

4 Trust Inference Algorithm Based on the Proposed Framework

A trust inference problem is a triple $(TN, n0, n_\infty)$ where TN is the trust network or web of trust. It is, as described in section 1, a directed labeled graph in which the vertexes denote entities and the label of an edge $v_i v_j$ signifies the value of direct trust the entity I has in the entity j. n_0 and n_∞ are the source and the target nodes in TN, respectively. A solution to a trust inference problem is a trust value from the interval [0,1] that describes the amount of trust the source has in the target. If there is no solution, then the amount of trust of the source in the target remains unknown [8].

If the source node has some experience of interacting with the target, it can usually evaluate the target's trustworthiness level directly and the result of this evaluation is reflected in the trust network using a direct edge (arc) from source to target. In such a case, the solution to the trust inference problem is often simply the label of that edge. However, the difficulty of trust inference problem arises when the source node has no experience of prior interaction with the target node. For such a case, it is necessary to find ways of estimating the trust value indirectly based on the recommendations from intermediate nodes and other ways.

In this section, first the algorithm for calculating the inferred trust is being proposed. Since the confidence used in this algorithm is estimated based on a novel multi-measure approach, a description of this approach will also be provided.

4.1 Trust Estimation Algorithm

As was also discussed before, trust interval multiplication and summation operators refer to computing propagated and aggregated confidence-aware trust, respectively. Therefore, the two operators can be combined in order to estimate the trust from a source to a target in the web of trust. For example, to estimate the trust from node S to node D in the web of trust in Figure 1, we can compute

$$TI_{SD} = TI_{SA} \otimes TI_{AB} \otimes TI_{BD} \oplus TI_{SC} \otimes TI_{CD}.$$

Having this in mind, the algorithm proposed here to find the solution to trust inference problem can be represented as in Algorithm 1. To estimate the value of trust from the source node (s_0) to the target node (s_∞), one should find all paths (trust chains) from source to target. In the same vein, in order to solve the problem of dependent paths, first the approach based on edge splitting is used as suggested in [17]. The function CanonicaliseTrustNetwork performs this task and returns the canonical trust network, CTN. As explained in [17], optimal splitting leads to removing the least certain paths from trust network.

Then we should determine the propagated trust through each path (TI_{path}), and finally compute the resultant of the values obtained from different paths as inferred trust (TI_{inf}). In each path, the multiplication operator stated in (13)-(15) is utilized for trust propagation. TIpath is initialized with [1,1] i.e. the left identity element of multiplication operator. Then the propagated trust interval (TI_{path}) is multiplied by trust interval of each edge in the path (TI_{ij}).

Algorithm 1 Trust inference

Input:
Trust Network (TN),
source node (n_0),
target node ($n\_$)
Output:
Inferred trust which describes the amount of trust that the source has in the target (TI_{inf})

```
CTN = CanonicaliseTrustNetwork(TN,n0,n_)
TIinf = [0,1]
for all paths p in CTN do
    TIpath = [1,1]
    for all edges ninj in the path p do
        TIpath = TIpath ⊗ TIij(using(12) − (14))
        TIinf = TIinf ⊕ TIpath(using(15) − (17))
    end for
end for
return TIinf
```

To compute the final trust, TI_{inf}, as the resultant of the trust intervals obtained from different paths, the summation operator described in (16)-(18) is used. The identity element of this operation is [0,1]. Accordingly, the TI_{inf} is initialized with [0,1].

4.2 Confidence Estimation Approach

The value of confidence used in the algorithm may be achieved directly. However, in many cases the trust network contains only the values of trust. In such cases, the values of confidence should be estimated in some way indirectly. Several studies including [7, 8, 19] use similarity measures as an estimation of the confidence the source has in an appraiser (intermediate) node. In fact, the degree of similarity between the opinions of the source and an appraiser in the cases where opinions of both are available, is considered as a measure of the confidence of the source node in the appraiser's recommendations.

Our approach to estimating the confidence, on the other hand, uses four measures:

(1) *Expertise Confidence* (*ExpC*): based on the expertise level of the appraiser,
(2) *Source Confidence* (*SrcC*): based on the level of similarity between the appraiser's and the source's opinions about other nodes,
(3) *Society Confidence* (*SocC*): based on the level of similarity between the appraiser's and the average of the society's opinions about the destination node,
(4) *Freshness Confidence* (*FrsC*): based on the time passed from the moment the opinion was offered.

For a node i, *ExpC* can be calculated using (41).

$$ExpC_i = \left(1 - \frac{1}{n+1}\right)\frac{\sum_{j=1}^{n} E_{j,i}}{n} \quad (41)$$

Where E_j, i is the value of trust node j has in node i's expertise, and n is the number of reporting nodes. SrcCi may be estimated using (42).

$$SrcC_i = (1 - \frac{1}{m+1})\frac{\sum_{j=1}^{m} |T_{src,j} - T_{i,j}|}{m} \quad (42)$$

in which Tsrc,j and T_i, j are the trust ratings for node j, according to source and node i, respectively, and m is the number of the nodes they both rated.

Similarly SocCi. may be estimated using (43) below:

$$SocC_i = \left(1 - \frac{1}{p+1}\right)\frac{\sum_{j=1}^{p} |T_{i,dest} - T_{j,dest}|}{p}, \quad (43)$$

where T_i,dest and T_j,dest are trust ratings for destination node, according to nodes i and j, respectively, and p is the number of nodes that have rated the destination node.

Finally, (44) is suggested for estimating FrsCi.

$$FrsC_i = (1 - \lambda)^{\Delta t} \quad (44)$$

where Δt is the time passed since the appraiser i has given its opinion, and $0 \leq \lambda < 1$ is the freshness (recency) impact factor.

Now, these four types of confidence are combined to obtain the overall confidence:

$$C_i = FrsC_i(\frac{n.ExpC_i + m.SrcC_i + p.SrcC_i}{n+m+p}) \quad (45)$$

5 Experiments and Results

To evaluate the accuracy of the proposed solution, the method was applied to the well-known datasets of Advogato and Epinions together with some other methods. The former dataset contains information of trust among the members of an internet community of programmers and one of its aims is to provide a source for trust experiments. The latter is a web of trust, obtained from the general consumer review site Epinions.com, where the users are encouraged to not only rate the items but also explicitly express their trust on other users. Several other works including [4, 5, 28] used these datasets for evaluating their algorithms, as well.

However, these datasets contain no information on confidence and, to the best of our knowledge, there is no other trust dataset which contains such information. Accordingly, the approach described in Section 4.2 was used for confidence estimation.

To evaluate and compare the accuracy of the proposed method, the leave-one-out technique, which is a common validation method in trust research works, was employed. In this method, since any pairs of nodes, say v_i and v_j, which direct trust of v_i in v_j is available, we also calculate the indirect (estimated) value of trust from v_i to v_j, using each algorithm and consider the correlation and mean of absolute error (MAE) for both the direct and indirect trust as measures of the algorithm accuracy.

Thus, all of the pairs (i, j) in the trust network, between which the value of direct trust was available, were found,. In each case, we calculated the estimated value of trust from n_i to n_j in the form of a trust interval using the proposed algorithm. In order to draw comparisons between the results and the ones obained by the other methods, we then extracted the explicit value of trust from trust interval using (8). On the other hand, we calculated the estimated trust of each node ni in node nj ,using TidalTrust [6], SUNNY [7], and FIRE [9] methods independently. As mentioned earlier, TidalTrust is a well-known trust inference algorithm, and SUNNY and FIRE are among the most important trust models addressing the concept of confidence.

5.1 Experiments on Advogato

The dataset of Advogato is a text file including about 71000 lines of data, containing information on trust among about 14000 programmers. Each programmer has stated the value of his/her trust in another programmer in the terms of one of the words *Apprentice*, *Journeyer*, or *Master*. Mapping these words into the numbers in the range [0,1] is left to the user. We tried different mappings as follows: the values 0, 0.1, 0.2, and 0.3 were considered for *Apprentice*, 0.4, 0.5, and 0.6 for *Journeyer*, and 0.7, 0.8, 0.9, and 1 for *Master*, resulting in totally $4 \times 3 \times 4 = 48$ different mappings. The first of these mappings, for instance, is represented by <0, 0.4, 07>.

Having tested the four algorithms with each mapping , it was found that,

(1) The proposed algorithm provides lower MAE and higher correlation values comparing to the other algorithms for all mappings.
(2) The mappings with which each algorithm works best (in terms of minimizing the MAE) are either <0.2, 0.5, 0.8> or <0.2, 0.5, 0.9>. Hence, the results of the comparison will be reported based on these two mappings.

It should be noted that since the data in Advogato do not include the time point when the rating is created, we ignored $FreshnessConfidence(FrsC)$ measure in confidence estimation in the experiments on Advogato. To this end, we may let $\lambda = 0$ (or equivalently $\Delta t = 0$) in (44) obtaining $FrsC_i = 1$ for every opinion. In fact, we temporarily reduce the confidence estimation approach to a static one where only the other measures -rather than time- play a role.

We ran our method together with the other above-mentioned algorithms on the dataset and computed the MAE and correlation comparing to real (direct) trust values, each time. The results are summarized in Table 4.

As can be observed in Table 4 , the mean value of absolute error in our method is remarkably less than the values in TidalTrust, FIRE, and SUNNY using each of the two mappings. On the other hand, the correlation among indirect and direct trust values has been increased when compared to the other algorithms.

Table 4. Comparison of the proposed method with other algorithms using Advogato dataset.

	Mapping <0.2,0.5,0.8>		Mapping <0.2,0.5,0.9>	
	MAE	**correlation**	**MAE**	**correlation**
TidalTrust	0.052	0.86	0.059	0.82
FIRE	0.070	0.81	0.067	0.82
SUNNY	0.046	0.88	0.053	0.84
Proposed Method	0.037	0.92	0.041	0.90

For comparison purposes, the results of a different approach are represented in Table 5. Here, the results of trust estimation have been converted back to the three-level categorical space and the rate at which each algorithm estimated the correct/incorrect categories have been also computed. Different types of incorrect estimates are shown in separate rows in the table, where A, J, and M stand for *Apprentice*, *Journeyer*, and *Master*, respectively. The row $A \rightarrow J$, for instance, indicates the rate of cases where the real trust category is *Apprentice*, but the algorithm estimates it as *Journeyer*, incorrectly. The other rows can be interpreted in a similar way.

As can be viewed from Table 5, the rate of correct estimates by the proposed method is higher comparing to the other algorithms. Besides, the rate of wrong estimates by this method is less than the other algorithms, almost for all different types of incorrectness.

Therefore, it can be concluded that this new method outperforms the other algorithms using all the 48 possible mappings. However it may not be the case if an unreasonable mapping, e.g. <0, 0.9, 1>, is used.

Table 5. Rates of correct and different types of incorrect estimates on Advogato using different algorithms.

		Mapping <0.2,0.5,0.8>	Mapping <0.2,0.5,0.9>
TidalTrust	**Correct**	**0.931**	**0.918**
	$A \rightarrow J$	0.014	0.017
	$A \rightarrow M$	0.004	0.005
	$J \rightarrow A$	0.013	0.013
	$J \rightarrow M$	0.013	0.019
	$M \rightarrow A$	0.007	0.006
	$M \rightarrow J$	0.018	0.022
FIRE	**Correct**	**0.903**	**0.912**
	$A \rightarrow J$	0.020	0.018
	$A \rightarrow M$	0.007	0.003
	$J \rightarrow A$	0.017	0.014
	$J \rightarrow M$	0.017	0.016
	$M \rightarrow A$	0.011	0.012
	$M \rightarrow J$	0.025	0.025
SUNNY	**Correct**	**0.946**	**0.923**
	$A \rightarrow J$	0.012	0.015
	$A \rightarrow M$	0.001	0.004
	$J \rightarrow A$	0.012	0.013
	$J \rightarrow M$	0.012	0.018
	$M \rightarrow A$	0.004	0.006
	$M \rightarrow J$	0.013	0.021
Proposed Method	**Correct**	**0.960**	**0.947**
	$A \rightarrow J$	0.008	0.010
	$A \rightarrow M$	0.001	0.005
	$J \rightarrow A$	0.009	0.009
	$J \rightarrow M$	0.007	0.011
	$M \rightarrow A$	0.004	0.002
	$M \rightarrow J$	0.011	0.016

5.2 Experiments on Epinions

The dataset of Epinions consists of 49,288 users and 487,183 trust statements. Each trust statement contains the IDs of truster and trustee, the value of trust, and the time point when the rating is created. The last field is important for us and one of our major reasons to choose this dataset, as our approach to confidence estimation requires the time parameter, and to the best of our knowledge, other well-known trust datasets do not include the time field for each trust statement.

Therefore, different values for the *freshness impact factor* (λ) were tried and it was found that the optimum value for this parameter is $\lambda = 0.004$. However, the optimal value for λ depends in general on several factors including the context of trust, the society, and the unit of time. However as will be shown, our solution outperforms the other methods, even if we consider $\lambda = 0$, i.e. absolutely ignoring the impact of time.

Similar to the experiments on Advogato, we calculated the estimated trust of each node n_i in node n_j, using TidalTrust, SUNNY, and FIRE algorithms independently.

Once again, we computed the mean of absolute error (MAE) and correlation coefficient among each method's results and direct trust values. The results are illustrated in Table 6.

As Table 6 shows, the mean of absolute error in our method with $\lambda = 0$, is 0.046 which is less than the values in TidalTrust, FIRE, and SUNNY. In addition, it is observable form the table that the correlation among indirect and direct trust values has been increased to 0.86. This implies that our method provides more accuracy even if we just consider the three other measures we explained in Section 4.2 rather than time, in confidence estimation.

The last row of the table signifies that when we consider the optimal value we have found for λ, that is 0.004 as mentioned before, the accuracy of our method is even higher. In this case, MAE is reduced to 0.042, and the correlation is increased to 0.90.

Table 6. Comparison of the proposed method with other algorithms using Epinions dataset.

	MAE	**Correlation**
TidalTrust	0.060	0.81
FIRE	0.074	0.79
SUNNY	0.048	0.82
Proposed Method with $\lambda = 0$	0.046	0.86
Proposed Method with $\lambda = 0.004$	0.042	0.90

6 Conclusion and Future Work

In the present paper, first a framework was introduced for integrated representation of trust and confidence using intervals, as well as operations on trust intervals. In this regard, some properties of the proposed operations were analyzed and proved. In addition, an approach to confidence estimation was aslo proposed considering four measures, which was shown to improve the accuracy of confidence-aware trust computation.

The notation and operations proposed here, not only represent the trust along with confidence in a more intuitive way, but also provide a good approach to combine opinions confirming or contradicting one another.

However, the effect of other measures in confidence estimation such as appraiser's distance from the source and conflicts among opinions are intended to be investigated in future. It may cause the trust interval system to include summation and/or multiplication reverse for trust intervals and therefore, convert the system into a more advanced algebraic system. other future studies will include invesigation of the applications of intervals in analyzing the sources of uncertainty in trust management, eliminating subjectivity from trust assessment, and clustering nodes of the web of trust.

References

[1] H. Shakeri and A. G. Bafghi. Computing trust resultant using intervals. *In Proceedings of the 8th International ISC Conference on Information Security and Cryptology (ISCISC'11),* pages 15-20.FUM, Mashhad, Iran, 2011.

[2] H. Shakeri and A. G. Bafghi. Propagation of trust and confidence using intervals. *In Proceedings of the 6th International Conference for Internet Technology and Secured Transactions (ICITST 2011),* pages 436-441. Khalifa University, Abu Dhabi, UAE, 2011.

[3] D. Olmedilla, O. Rana, B. Matthews, and W. Nejdl. Security and trust issues in semantic grids. *In Proceedings of the Dagsthul Seminar, Semantic Grid: The Convergence of Technologies,* no. 05271, 2005.

[4] P. Massa and C. Hayes. Page-rank: Using trusted links to re-rank authority. *In Proceedings of the 2005 IEEE/WIC/ACM International Conference on Web Intelligence (WI'05),* pages 614-617.Washington DC, USA, 2005.

[5] H. Shakeri and A. G. Bafghi. RTBIMS: Accuracy enhancement in iterative multiplication strategy for computing propagated trust. *In Proceedings of the 8th International ISC Conference onInformation Security and Cryptology (ISCISC'11),* pages 9-14.FUM, Mashhad, Iran, 2011.

[6] J. A. Golbeck. Computing and applying trust in web-based social networks. *Ph.D. Dissertation,* University of Maryland, College Park, 2005.

[7] U. Kuter and J. Golbeck. SUNNY: A new algorithm for trust inference in social networks using probabilistic confidence models. *In Proceedings of the 22nd National Conference on Artificial Intelligence, British Columbia, Canada,* pages

1377-1382. 2007.

[8] U. Kuter and J. Golbeck. Using probabilistic confidence models for trust inference in web-based social networks.*ACM Transactions on Internet Technology,* 10(2):Article 8, 2010.

[9] T. Huynh, N. Jennings, and N. Shadbolt. An integrated trust and reputation model for open multi-agent systems, *Autonomous Agents and Multi-Agent Systems,* 13:119-154, 2006.

[10] L. Ding, P. Kolari, S. Ganjugunte, T. Finin, and A. Joshi. Modeling and evaluating trust network inference. *In Proceedings of the 7th International Workshop on Trust in Agent Societies at AAMAS,* 2004.

[11] J. Sabater. Trust and reputation for agent societies. *Ph.D. Thesis,* Universitat Autonoma de Barcelona, 2003.

[12] W. Teacy, J. Patel, N. Jennings, and M. Luck. Travos: trust and reputation in the context of inaccurate information sources. *Journal of Autonomous Agents and Multi-Agent Systems,* 12(2):183-198, 2006.

[13] . Saadi, J. M. Pierson, and L. Brunie. Authentication and access control using trust collaboration in pervasive grid environment. *In Proceedings of the International Conference on Grid and Pervasive Computing (GPC 2007),* 2007.

[14] O. Hasan, L. Brunie, and J. M. Pierson. Evaluation of the iterative multiplication strategy for trust propagation in pervasive environments. *In Proceedings of ICPS'09,*London, United Kingdom, 2009.

[15] Y. Wang and M. P. Singh. Trust representation and aggregation in a distributed agent system. *In Proceedings of 21st National Conference on Artificial Intelligence (AAAI),* pages 1425-1430. Boston, MA, USA, 2006.

[16] A. Jøsang and S. G. Knapskog. A metric for trusted systems. *In Proceedings of the 21st National Security Conference,* pages 16-29. Arlington, Virginia, USA, 1998.

[17] A. Josang and T. Bhuiyan. Optimal trust network analysis with subjective logic. *In Proceedings of the 2nd International Conference on Emerging Security Information, Systems and Technologies,* pages 179-184. Cap Esterel, France, 2008.

[18] A. Das and M. M. Islam. SecuredTrust: A dynamic trust computation model for secured communication in multi-agent systems. *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING,* 9(2):261-274, 2012.

[19] J. Hu, Q. Wu, and B. Zhou., FCTrust: A robust and efficient feedback credibility-based distributed P2P trust model. *In Proceedings of the 9th International Conference for Young Computer Scientists,* pages 1963-1968. Zhang JiaJie, China, 2008.

[20] B. Khosravifar, J. Bentahar, M. Gomrokchi, and R. Alam. CRM: An efficient trust and reputation model for agent computing, *Journal of Knowledge-Based Systems,* 30:1-16, 2012.

[21] J. S. Chang and H. J. Wong. Selecting appropriate sellers in online auctions through a multi-attribute reputation calculation method. *Journal of Electronic Commerce Research and Applications,* 10:144-154, 2011.

[22] X. Qiu, L. Zhang, S. Wang, and G. Qian. A trust transitivity model based on Dempster-Shafer theory. *Journal of Networks,* 5(2): 1025-1032, 2010.

[23] Y. A. Kim and H. S. Song. Strategies for predicting local trust based on trust propagation in social networks. *Journal of Knowledge-Based Systems,* 24(8):1360-1371, 2011.

[24] J. Urbano, A. P. Rocha, and E. Oliveria. Computing confidence values: Does trust dynamics matter?. *In Proceedings of EPIA'09,* Portugal, 2009.

[25] J. Weng, Z. Shen, C. Miao, A. Goh, and C. Leung. Credibility: How agents can handle unfair third party testimonies in computational trust models. *IEEE TKDE,* 22(9):1286-1298, 2010.

[26] Y. Wang and L. Li. Two-dimensional trust rating aggregations in service-oriented applications, *IEEE TRANSACTIONS ON SERVICES COMPUTING,* 4(4):257-271, 2011.

[27] W. Ping, Q. Jing, and Q. Y. Hui. A computation al trust model with confidence in unstructured P2P systems. *In Proceedings of 2009 Joint Conferences on Pervasive Computing (JCPC 2009),* pages 451-454. Tamkang University, Taipei, Taiwan, 2009.

[28] A. G. Bafghi and H. Shakeri. Improving iterative multiplication strategy in estimating propagated trust using similarity measure and ant colony optimization. *In Proceedings of the 16th Annual CSI Computer Conference, pages 374-379.* Sharif University, Tehran, Iran, 2011.

Hassan Shakeri received his B.Sc. and M.Sc. degrees in computer engineering from Ferdowsi University, Mashhad, Iran, in 1995, and Sharif University of Technology, Tehran, Iran, in 1997, respectively. Currently, he is with the Department of Information Technology, Islamic Azad University of Mashhad. He is also a PhD student in computer engineering at Ferdowsi University of Mashhad. His research interests include trust management, computer system security, and natural language processing. He has published more than 20 papers in national and international conferences and journals.

Abbas Ghaemi Bafghi received his BS degree in Applied Mathematics in Computer from Ferdowsi University of Mashhad, Iran in 1995, and MS degree in Computer engineering from Amirkabir (Tehran Polytechnique) University of Technology, Iran in 1997. He received his PhD degree in Computer Engineering from Amirkabir (Tehran Polytechnique) University of Technology, Iran in 2004. He is member of Computer Society of Iran (CSI) and Iranian Society of Cryptology (ISC). He is an assistant professor in Department of Computer Engineering, Ferdowsi University of Mashhad, Iran. His research interests are in cryptology and security and he has published more than 70 conference and journal papers.