International Journal of Information Science and Intelligent System, 3(1): 73-90, 2014

A Layer Model of a Confidence-aware Trust Management System

Hassan Shakeri [1, *], Abbas Ghaemi Bafghi [2]

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

Received: 20 October 2013; Accepted: 11 December 2013

Abstract

Recently the concept of confidence has received a remarkable attention in trust research area. This paper introduces an integrated layer model of a confidence-aware trust management system which can be useful in providing a global view of these systems. It provides an abstract view of the main components of the system, their functions, and the relations among them. We also report and analyze the results of experiments carried out on the model using the well-known trust dataset of Epinions.

Keywords: Trust; Trust management; Confidence; Layer model

1. Introduction

Trust management has obtained 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.

According to [4], trust management is "the activity of creating systems and methods that allow relying parties to make assessments and decisions regarding the dependability of potential transactions involving risk". To this end, there exist several issues that should be addressed in a trust management system, including appropriate representations of trust opinions, calculating the trustworthiness level of an entity based on the outcomes of direct interactions with it, operators for estimating indirect trust based on the recommendations from intermediate nodes (trust propagation) and computing the resultant of trust opinions (trust aggregation), and appropriate decisions based on the final trust assessment.

* Corresponding author. Tel.: 98-9155138798
E-mail address: Hassan.Shakeri@gmail.com (Hassan Shakeri).

In a society (of people or systems) we may consider a web of trust, a directed graph in which the vertices denote the entities and the edge labels reflect trust opinions, i.e. the trust each entity maintains in every other entity. A sample web of trust is shown in Fig. 1.

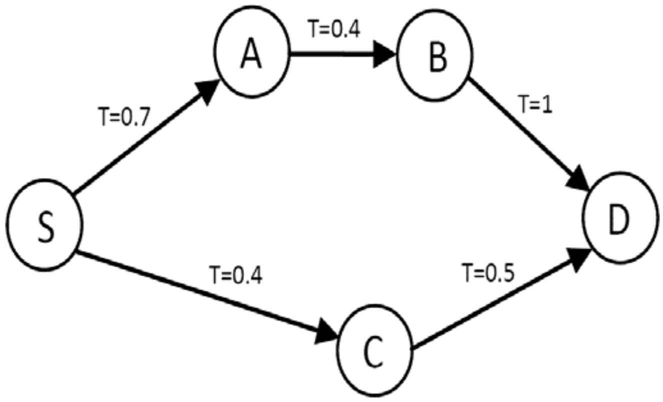

Figure 1. A sample web of trust

Let's denote the propagation and aggregation operators with ⊗ and ⊕, respectively. In Fig. 1, the source node, S, has two trust chains towards the destination (target) node, D. Each chain includes some edges. The indirect trust from S to D may be computed as SA⊗AB⊗BD⊕SC⊗CD.

Recently, on the other hand, the concept of confidence has received a remarkable attention in trust research area. Confidence is a metric that represents the accuracy of the trust values[27]. In other words, 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. It is important to have not only an accurate estimate of trust among nodes, but also a measure of confidence in the estimated value of trust.

As an example, consider the web of trust in Fig. 2 that is the one in Fig. 1, when each trust value is associated with the level of confidence. The label on the edge SA, for example, 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 may be interpreted in a similar way. Now, to estimate the trust S may have in D, it is important to know how S should apply the confidence labels in trust propagation in each chain, and then how it should consider the confidence values of each chain to aggregate the trust values obtained from the two chains, and how confident this final S's judgment is. In other words, ⊗ and ⊕ operators should take into account both the trust and confidence values. Also in the higher level, a trust value can help better decision making, when accompanied with the confidence measure.

In the rest of this paper, we always take into account the confidence along with trust, and by *opinion*, we mean *confidence-aware trust opinion.*

Many researchers are working in the field of trust management. However, each research work usually addresses a specific issue. On the other hand, an integrated model of a trust management system can be useful in providing a global view of the system. One of the main objectives of this paper is introducing such a model. This model is a layered one which provides an abstract view of the main components of a trust management system, their functions, and the relations among them. It is a confidence-aware model, i.e. considers the concept of confidence in all layers. The proposed model helps better understanding of different problems in the field, in sense of their positions in the whole system. Also it includes well-defined interfaces between layers which facilitate the combination of the solutions addressing different issues of trust management. We will describe the advantages of the proposed model in more details in section 6.

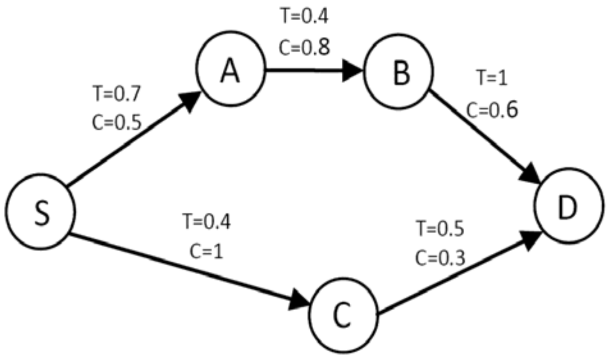

Figure 2. A sample web of trust including confidence values

The rest of this paper is organized as follows: Section 2 describes the related work. In section 3, we provide an overview of our proposed model including its layers and units and their functions. Then in section 4, we describe our suggested data format and different representations of trust opinions best suitable for each layer, and in section 5, we suggest the interfaces between the adjacent layers/sub-layers. In section 6, the main advantages of the proposed model will be discussed. We report the results of the experiments conducted on the proposed model in section 7. Finally we conclude in section 8.

2. Related Work

A variety of research works have been done in the area of trust management.

Some works including [9, 16, 17] address the factors of trust in specific domains. Many other works focus on or include the mapping between the evidence space and the trust space, i.e. evaluating the direct trust value based on the observations and evidences from the target behavior. For example, in [13, 19, 25] the trustworthiness is evaluated using the corresponding formulas from the Beta distribution, which is a common approach to model the evidence space. On the other hand, some works including [6, 10] use Dirichlet distributions to measure the level of trust among nodes according to their mutual experience. In [14], we proposed a time-variant method that considers freshness, expertise level and two similarity measures in confidence estimation.

There are also several works dealing with indirect trust estimation. We refer, for instance, to [23, 30] as well-known works in this area.

Some works in the area of trust, propose trust-based approaches to decision making in specific domains. For example, [11, 20] use the concept of trust in wireless sensor networks and [18] proposes a support tool for e-commerce environment to assist users in choosing sellers when using auction sites.

The security threats that can compromise trust management systems are addressed in some works. In [12], some of the most important threats are described and analyzed, and some recommendations are proposed to face them.

Some works address the problem of subjectivity in trust estimation or trust-based decision-making. For instance, Hasan et al. in [22] use a method for eliminating subjectivity from trust recommendations. [8, 21] address the concept of *disposition to trust* and its importance in trust management. Disposition to trust is the inherent propensity of an individual to trust or distrust others.

On the other hand, there exist research works which take into account the impact of confidence or similar concepts in each of the above fields. Some works, including FIRE[24], SecuredTrust[1], CRM[5], and SUNNY[26] have paid attention to the parameters and estimation of confidence.

Some other works have focused on representation of confidence and/or approaches to propagation and aggregation of confidence-aware trust. One of the first works in this area is Jøsang and Knapsdog's one[2]. They represent an opinion on trust by a triple $\{b, d, u\}$ in which b, d and u designate belief, disbelief and uncertainty, respectively. They also introduce a subjective logic with operators for opinion propagation and aggregation. In [9, 15], an interval representation is proposed as a clearer and more intuitive approach to representing trust opinions, comparing to Jøsang et al.'s triple.

Some works use Dempster-Shafer theory to deal with confidence in computing of trust. For example in [28], trust opinions are represented as mass assignments in DST and then they are combined using Dempster's rule of combination to obtain the aggregated opinion.

Some papers including [6, 24, 29] propose some kinds of integrated models of trust, i.e. models considering different issues related to trust management. However, our integrated model to be proposed in this paper differs from those in that it is a layer model with well-defined functions of and interfaces between the layers.

3. An Overview of the Proposed Layer Model

In this section, we provide an overview of our proposed model including its layers and units and their functions. Then in sections 4-6, we describe and discuss more details relating to the model.

An overall view of our layer model for confidence-aware trust management system is shown in Fig 3. As the figure shows, this is a four-layer model with two cross-layer units. We provide a high-level description of the layers and cross-layer units in this section.

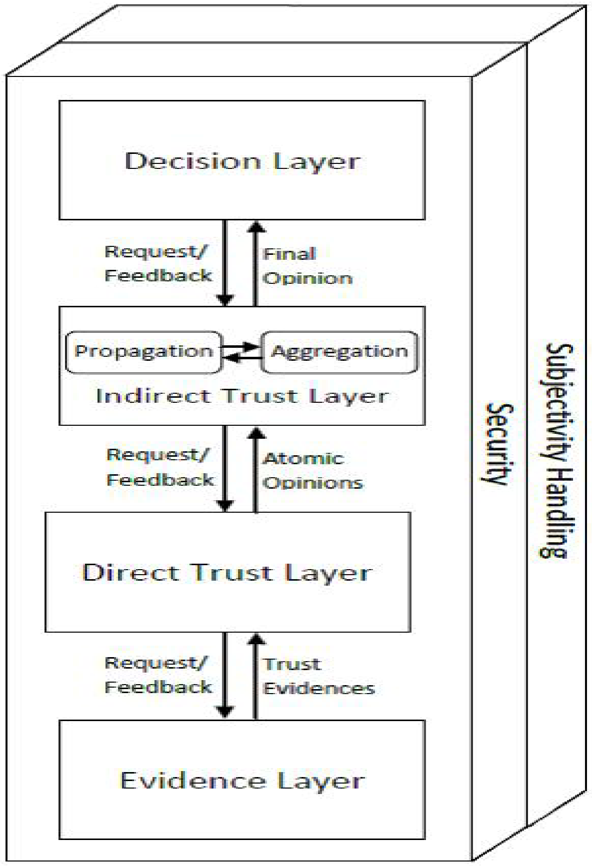

Figure 3. The proposed layer model for confidence-aware trust management systems

The first layer of the model is the e*vidence layer.* This layer is concerned with gathering the appropriate *evidences* -which can be used in estimating direct trust value-, and passing them to the direct trust layer. The most common evidences are the ones obtained as the result of interaction with the trustee entity. However, there also exist different evidences like the popularity of a brand, the guarantees given by the trustee party, etc.

The main functions of the evidence layer include

- Acquiring the values of the parameters specified by the direct trust layer, by monitoring the interactions with the trustee party, requesting from other entities, etc.,
- Estimating the uncertainty level of the acquired values,
- Providing the direct trust layer with the results of data acquisition, including the parameter values, uncertainty level, time of the interaction, etc.

The second layer is the *direct trust layer*, which requests the evidence layer for the appropriate evidences, and upon receiving them, estimates the direct trust value and the confidence in that value. These trust and confidence values form the *atomic opinions*, which are passed to the upper layer, i.e. indirect trust layer.

The main functions of the direct trust layer are as follows:

- Identifying the appropriate parameters for direct trust estimation,

- Requesting the evidence layer for the evidences relating to the identified parameters,
- Estimating atomic opinions reflecting both the trust value in the target entity, and the confidence level in this estimation,
- Reporting the atomic opinions to the indirect trust layer.

We may consider a web of trust like the one in Fig. 2, as the result of the direct trust layer.

The third layer of the model, the *indirect trust layer,* is responsible for estimating confidence-aware trust opinions, based on the information provided by third-party entities. It includes two sub-layers: The *propagation sub-layer*, at a moment, receives two opinions as inputs and computes the result of propagation. The *aggregation sub-layer*, on the other hand, receives two opinions at a time, and aggregates them.

In fact, the propagation and aggregation sub-layers implement ⊗ and ⊕ operators, mentioned in section 1, respectively. The input to each of these sub-layers may be accepted either from the direct trust layer, the other sub-layer, or even the sub-layer itself. This latter option implies that we may calculate the result of propagating/aggregating more than two opinions, by repeatedly using the propagation/aggregation sub-layer.

As an example, to compute the final trust opinion from S to D, in Fig. 2, the propagation and aggregation sub-layers should be used to compute the following statement:

$SD=(((SA \otimes AB) \otimes BD) \oplus (SC \otimes CD))$

The output of the indirect trust layer is the *final confidence-aware trust opinion*, or *final opinion* for short, that is passed to the upper layer, i.e. decision layer.

The main functions of the indirect trust layer include

- Finding all the trust chains from the source node to the target node in the web of trust,
- Deciding on the statement (in terms of atomic opinions combined using ⊗ and ⊕ operators) to be computed,
- Computing the result of the specified statement, with proper ⊗ and ⊕ operators, which guarantee the expected properties for opinion propagation and aggregation,
- Reporting the result, i.e. final opinion, to the decision layer.
-

The last layer is the *decision layer*, which addresses the strategies, methods and considerations related to decision making based on the received confidence-aware trust opinion. In other words, this layer is concerned with the decision to trust or not to trust. This is an application-sensitive issue and may be supervised by human managers. This layer also analyses the outcome of decisions and actions, and sends the feedback to the lower layers, which may lead them to revise their methods or tune some parameters.

The main functions of the decision layer include

- Requesting the lower layer for final opinion on the target node(s),

- Considering the conditions and circumstances, and making proper decision to trust or not to trust the target node(s),
- Creating the feedback of made decisions, and sending it to the lower layers.

As illustrated in Fig. 3, the proposed model includes two cross-layer units. That is because there are functions, i.e. security and subjectivity handling, which are not tied to a given layer, but they can affect all the layers.

The security unit is responsible for securing the trust management system against potential attacks. There are different possible security threats in different layers that can compromise the system, including bogus evidences, unfair recommendations, collusion, etc., and the security unit should prevent these threats or at least limit their impacts on the system.

On the other hand, subjectivity is another problem in different layers where the human opinions play role. Different aspects of human subjectivity may reduce the accuracy of estimations or correctness of decisions. For instance, two individuals may have different levels of *attitude to trust* or different *perception* of the same trust value, thus the recommendations passed between them, may lose its real meaning, unless the subjectivity is eliminated. The subjectivity handling unit is responsible for this elimination.

4. Data Format and Opinion Representations

In the evidence layer, the evidences on the trustee's behavior, history, competence, etc. are gathered and passed to the upper layer inside *evidence data packets* (*EDPs*). Two types of evidences may be considered, for each of which we suggest a different type of EDP:

Interaction Evidence: This type of evidence reflects the results of a direct interaction with the trustee entity. We suggest *interaction evidence data packet* (*IEDP*) illustrated in Fig. 4(a) for this type of evidence. The field *Time* depicts the time of the interaction. Each pair (Val_i, $Cert_i$) shows the value of the trust parameter P_i and the certainty level related to that value.

General Evidence: This type of evidence helps estimating the trustworthiness level of the trustee based on the *signs* rather than the outcomes of direct interactions. These signs include the trustee's popularity, guarantees, credentials, rank in a specific ranking, belonging to a given group, etc. We suggest *general evidence data packet* (*GEDP*) illustrated in Fig. 4(b) for this type of evidence. Again, *Time* depicts the time relating to the sign, e.g. the date in which the popularity has been evaluated. The fields *ID* and *Value* denote the identifier and the value of the sign, respectively.

Time	Val_1	Val_2	...	Val_p
	$Cert_1$	$Cert_2$	...	$Cert_p$

(a)Format of IEDP

Time	*ID*
	Value

(b) Format of GEDP

Figure 4. Format of the evidence data packets

In the higher layers, on the other hand, the confidence-aware trust opinions are used. We suggest four different representations of opinion, each best suitable for a specific layer or sub-layer according to its functions. As we will explain, this enables different layers to deal with the features of the opinions from their own point of view. Before addressing these representations, we introduce two definitions: by atomic opinion, we mean an opinion given by an individual entity, i.e. a direct result of the direct trust layer. A single opinion is an opinion which is not a direct result of aggregating other opinions (it may be either an atomic opinion or the result of the propagation sub-layer).

Representation (a): <T, W>

This representation uses a pair of real numbers, <T, W>, in which $0 \leq T \leq 1$ denotes the trust value, and $0 \leq W \leq 1$ is called the weight of the opinion. We suggest this representation as the format of the output of direct trust layer, i.e. atomic opinions. W is a number between 0 and 1, depending on the reliability level of trust estimation, which depends in turn on the certainty level of the evidences received from the evidence layer.

Example 4.1 The opinion <0.6, 0.8> means that the trust in the target node is estimated at 0.6 based on the interactions of just one node with the target, and this estimation is reliable to the extent of 0.8.

The direct trust layer is responsible for generating atomic opinions in the form of <T, W>, based on the EDPs received from the evidence layer. Different approaches may be used in estimating the values of T and W. However, the values of the fields in EDPs, number of contributing evidences, and the weights assigned to different evidences, should be taken into account.

Representation (b): (T, C)

In this representation, an opinions is denoted by an ordered pair (T, C), in which $0 \leq T \leq 1$ is the value of trust, and $0 \leq C \leq 1$ is the level of confidence in that trust value. This representation is suggested as the format of input and output of the propagation sub-layer.

Example 4.2 If X estimates Y’s trustworthiness level at 0.8, and this estimation is confident to the extent of 0.5, we may represent this opinion with (0.8, 0.5).

Based on this representation, the ⊗ operator should be defined in such a way that values of T and C in operand opinions are properly considered in propagation. One suggestion is defining the propagation operator as follows.

$$(T_1, C_1) \otimes (T_2, C_2) = (T_P, C_P), \tag{1}$$

such that

$$T_P = T_2, \tag{2}$$

and

$$C_P = C_1.T_1.C_2, \tag{3}$$

where (T_P, C_P) denotes the final propagated opinion.

Representation (c): <T, W, S>

Based on this representation, the ⊗ operator should be defined in such a way that values of T and C in operand opinions are properly considered in propagation. One suggestion is defining the propagation operator as follows.

This is an extended form of the representation (a). This representation uses a triple of real numbers, <*T*, *W*, *S*>, in which *T* and *W* depict *trust* and *weight*, as in representation (a), except that here $W \geq 0$, i.e. the weight is not limited to 1, and may have any non-negative value. $S \geq 0$ is called the *weighted sum of square T values* and is used for estimating the consistency level of an opinion, as will be describe in section 5. This representation is suggested to be used in aggregation sub-layer of layer 3. For an atomic opinion (just received from the layer 2), *S* is equal to WT^2. For an aggregated opinion resulting from some atomic opinions, *T* is the weighted average of *T* components of the contributing opinions, and *W* and *S* are equal to the sum of their homonymous components in the contributing opinions. We will suggest these calculations in more details, in section 7.

Example 4.3 Consider the atomic opinion <0.8, 0.7> in the representation (a). It will be mapped to <0.8, 0.7, 0.448> in representation (c).

Example 4.4 If we aggregate two opinions <0.8, 0.6> and <0.3, 0.9>, the result will be <0.5, 1.5, 0.465>.

Based on this representation, the ⊕ operator should be defined in such a way that considers both the number and weights of the aggregated opinions and the level of consistency among them. One suggestion is the definition described in (4)-(7).

$$< T_1, W_1, S_1 > \oplus < T_2, W_2, S_2 > = < T_A, W_A, S_A >, \tag{4}$$

such that

$$T_A = \frac{W_1 T_1 + W_2 T_2}{W_1 + W_2}, \tag{5}$$

$$W_A = W_1 + W_2, \tag{6}$$

$$S_A = S_1 + S_2, \tag{7}$$

Where $<T_A, W_A, S_A>$ denotes the aggregated opinion.

Representation (d): [L, U]

This representation uses an interval to depict the concepts of trust and confidence, altogether. We name this interval a *trust interval*. $0 \leq L \leq 1$ and $L \leq U \leq 1$ are the lower and upper bounds of trust, respectively, and the width of the trust interval, i.e. *U*-*L*, is inversely related to the confidence, i.e. the narrower the trust interval is, the more confident the opinion is.

We suggest this representation to be used in the decision layer, as usually human user operates in this layer, and representing the trust opinion using an interval is more intuitive for human user, comparing to the previous representations.

Example 4.5 The trust interval [0.5, 0.8] depicts that the minimum value of trust is 0.5, and its maximum value is 0.8. On the other hand, the width of the trust interval is 0.3, which imply that the estimation is confident to the extent of 1-0.3=0.7.

Example 4.6 The trust interval [0.7, 0.7] means that the trust value is definitely 0.7, i.e. the minimum and maximum values of trust are both 0.7, and this estimation is absolutely confident.

Example 4.7 The trust interval [0, 1] provides no valuable knowledge about the trustworthiness of the target, as it was already obvious that the trust falls in the range 0 through 1. In other words, since the width of the trust interval is 1, the level of confidence should be considered 1-1=0.

On the other hand, from a trust interval [L, U], the expected value of trust may be computed as follows:

$$E = L + (U - L) * a, \tag{8}$$

where a is the *base rate*. Base rate determines how uncertainty shall contribute to the opinion's probability expectation value[3]. In the special case, when a is considered equal to 0.5, we have

$$E = \frac{L + U}{2}. \tag{9}$$

It means that the middle of a trust interval denotes the expected value of trust, when the base rate is considered equal to 0.5.

The decision layer is concerned with the decision making based on the received confidence-aware trust opinions, which are in the form [L, U]. Two main scenarios may be considered in this layer, which we call *threshold-based* and *sort-based* scenarios, respectively. In the threshold-based scenario, the source entity should decide to trust or not to trust a specific target entity. The decision may be made by comparing the final opinion received from the lower layer with a given threshold, say [L_{thr}, U_{thr}]. In the sort-based scenario, on the other hand, the source has received from the lower layer, final opinions about several entities, and should select (some of) the most trustworthy one(s) to trust and cooperate with. So a maximum-finding or sorting process is required.

In each of the two scenarios, an *order* should have been defined as the metric of comparison among confidence-aware trust opinions. Nature of such an order depends on the strategy defined for the decision layer, which in turn depends on the specific application and conditions. For example a threshold-based strategy may be based on the following rule:

If ($L \geq L_{thr}$ and $U \geq U_{thr}$) then
    Do trust
Else
    Do not trust

On the other hand, an order for comparing the opinions (and consequently the entities) in the sort-based scenario may be defined as follows:

$[L_1, U_1] \succcurlyeq [L_2, U_2] \equiv (L_1 \geq L_2$ or $(L_1 = L_2$ and $U_1 \geq U_2))$

The symbol $\succcurlyeq$ depicts the order, which is a total order relation.

5. Interfaces between Adjacent Layers/Sub-layers

In Fig. 3, the arrows between adjacent layers as well as the sub-layers of the layer 3, depict the flow of data and information among them. The downwards arrows show two types of data:

(1) The requests the upper layers send to their lower layers to ask for the wanted data/information. In fact, a lower layer sends the data/information to its upper layer either in response to a request from it, or when an event has been just occurred.

(2) The feedback which is a result of evaluating the impact of the previous received data/information. The feedback originates at the decision layer and in each lower layer, is considered as the basis of appropriate changes, and then passed to the lower layer, in a new format suitable for it.

The upwards and horizontal arrows, on the other hand, depict the main results prepared in each (sub-)layer, passed to its upper layer (or next sub-layer). However, the data and information used inside each of two adjacent (sub-)layers, differ either in nature or representation. So, we describe the interfaces between the layers and sub-layers, which mainly focus on the required conversions.

Interface between the layers 1 and 2

As mentioned earlier, the layer 1 prepares and passes EDPs to the layer 2. The two layers should first agree on the parameter list in IEDP, or the ID of the sign in GEDP.

Interface between layers 2 and 3

As mentioned in section 3, the layer 2, i.e. direct trust layer, produces an atomic opinion, and passes it to the layer 3, i.e. indirect trust layer. However, the format of the produced opinion in the layer 2 is $<T, W>$ (representation (a)), while the required format for the layer 3 is either (T, C) (representation (b)), or $<T, W, S>$ (representation (c)). So representation conversion is required.

To convert the representation (a) to (b), T remains unchanged. To determine C, we suggest (10).

$$C = 1 - e^{-\alpha W}, \tag{10}$$

where α>0, is the *individual entity weight factor*. In fact, (10) states how to map the weight of an atomic opinion to the confidence value, and α sets the level of confidence a completely reliable atomic opinion (W=1) provides, to $1-e^{-\alpha}$.

Conversion from representation (a) to (c) is simple. To do that, i.e. converting an opinion from the form $<T, W>$ to the form $<T, W, S>$, as mentioned in section 4, S should be considered equal to WT^2.

Interface between sub-layers of the layer 3

As we mentioned earlier in section 3, the propagation and aggregation sub-layers of the layer 3, may pass their result opinions to each other. However, they use different opinion representations, i.e. representations (b) and (c), respectively. So, conversion between these two is needed.

To convert the representation (c) to (b), *T* remains unchanged. To determine *C*, we first calculate the standard deviation among the values of *T* in the contributing atomic opinions, using (11).

$$\sigma = \sqrt{\frac{S - 2TS' + T^2 W}{W}}, \tag{11}$$

in which *S'* is the weighted sum of the *T* values, and simply obtained from (12).

$$S' = WT \,. \tag{12}$$

Then we compute the level of consistency among the contributing single opinions using (13).

$$Y = 1 - 2\sigma \,. \tag{13}$$

Note that since the *T* values are in the range [0, 1], the value of standard deviation falls in the range [0, 0.5], and according to (13), the value of *Y*, again falls in the range [0, 1].

Now, we calculate *C* using (14).

$$C = 1 - e^{-\alpha WY}, \tag{14}$$

where α is the individual entity weight factor, as in (10). Equation (14) states how to map the weight of an opinion and the consistency level among its composing opinions, to the confidence value. Fig. 5 shows this mapping for α=0.5, α=1, and α=2.

On the other hand, as we mentioned already in this section, an atomic opinion is a special case of opinions with *S* equal to WT^2. So for atomic opinions, the value of σ is obtained 0 from (11), and consequently the value of *Y* is obtained 1, from (13). In other words, (14) is a generalization of (10) for general opinions with the arbitrary values of *Y*.

We will show later in this section that in every single opinion, when represented in the form <*T*, *W*, *S*>, the value of *S* is equal to WT^2 (and so we have σ=0, and *Y*=1).

In the case of *Y*=1, we expect the function mapping *W* to *C,* to satisfy the following conditions:

$$f(0) = 0, \tag{15}$$

$$W > W' \Rightarrow f(W) > f(W'), \tag{16}$$

$$\lim_{W \to \infty} f(W) = 1 \,. \tag{17}$$

We can verify easily that this is the case in (14), and the mapping function is the same proposed in (10).

On the other hand, with given values for α and W, the value of C is increased with the increment of Y, i.e. the more consistent the composing opinions are, the more confident the result opinion will be. Fig. 6 shows the impact of Y on the confidence in the case of α=1 and W=2, for instance.

To convert the representation (b) to (c), on the other hand, *T* remains unchanged, again, and *W* and *S* should be obtained from (18) and (19), respectively.

$$W = \frac{-Ln(1-C)}{\alpha}, \tag{18}$$

$$S = WT^2. \tag{19}$$

Equation (18) may be considered as the reverse of (14), when *Y* is considered 1. The reason of considering *Y*=1, is that an opinion represented in the form (b) is a single opinion, so its consistency should be considered 1.

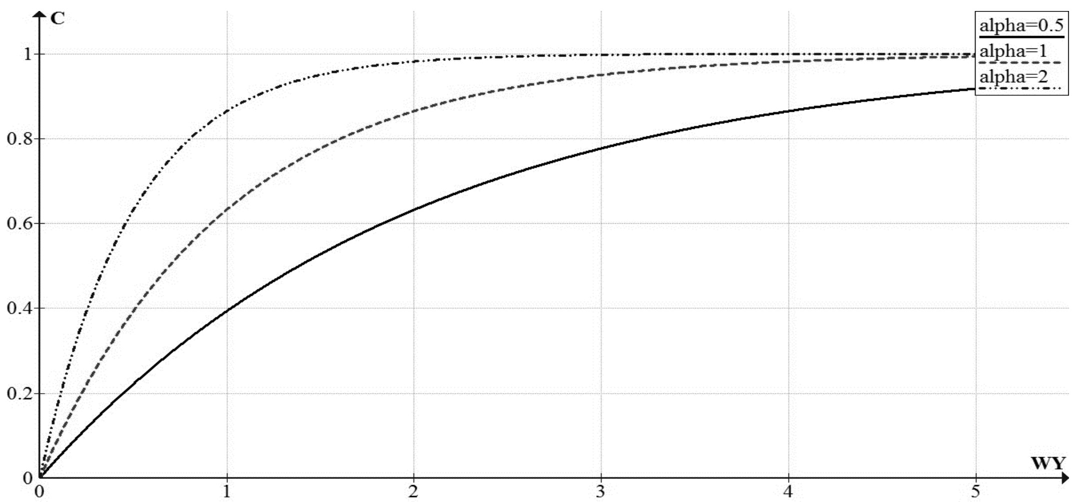

Figure 5. Mapping opinion weight and consistency level to confidence value Interface between the layers 3 and 4

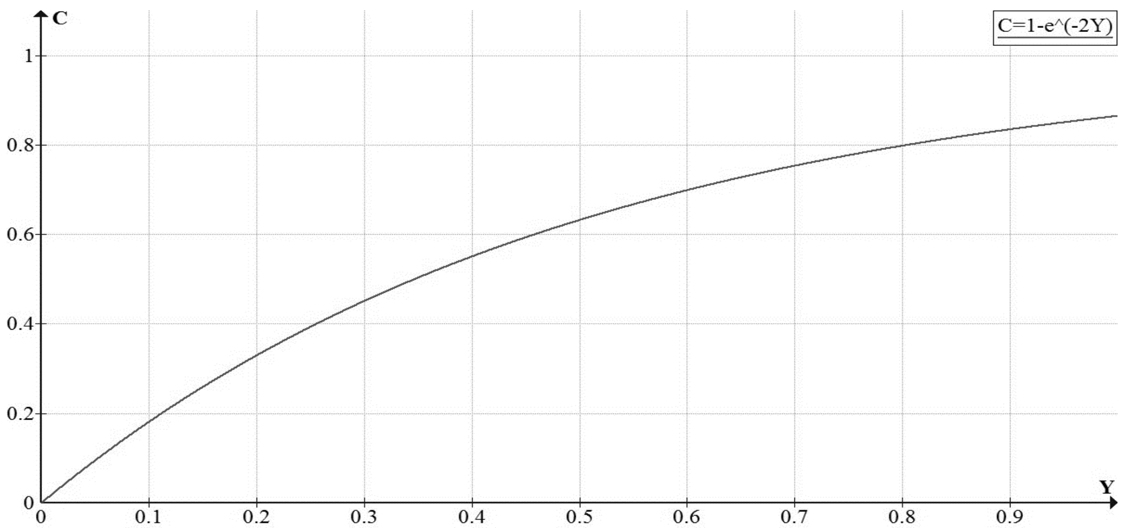

Figure 6. Impact of consistency on confidence level

As Fig. 3 shows, the result of the layer 3 (indirect trust layer) is the final trust opinion which is passed to the layer 4 (decision layer). However, any opinion in the layer 3 is represented either in representation (b) or (c), while the layer 4 expects to receive an opinion in representation (d). So, conversion is required at the interface of the two layers.

To convert the representation (b) to (d), we suggest (20) and (21).

$$L = C.T, \tag{20}$$

$$U = C.T + (1 - C). \tag{21}$$

We now explain how the lower and upper bounds of the trust interval are obtained: to determine the lower bound, we should consider the case when the base rate is a=0. C is the level of confidence and so 1-C is the value of uncertainty. Since trust is reported as T, the minimum of the confident trust is C*T. So the lower bound of the trust interval is obtained as follows.

$$\begin{aligned} L &= C.T + (1 - C).a \\ &= C.T + (1 - C).0 \\ &= C.T \end{aligned} \tag{22}$$

To determine the upper bound of the trust interval, on the other hand, we should consider the case when a=1. So we obtain the upper bound as follows.

$$\begin{aligned} U &= C.T + (1 - C).a \\ &= C.T + (1 - C).1 \\ &= C.T + 1 - C \end{aligned} \tag{23}$$

To convert representation (c) to (d), on the other hand, we may obtain the value of C from (14), and substitute it in (20) and (21), i.e. first map the opinion into representation (b), and then convert the result to the representation (d).

6. Advantages of Layered Model

Using a layer model for describing any system, which is inherently multi-layered, provides several advantages. The layered model of computer networks is a well-known example. Our layer model of a trust management system, inherits these advantages. In addition, it provides more benefits due to its special features. We mention some of the advantages provided by the model in the following.

(1) Providing a global view of the system. The proposed model affords an abstract view of the main components of a trust management system, their functions, and the relations among them, and hence helps better understanding of different problems in the field, in sense of their positions in the whole system. It considers the concept of confidence in all layers, as well.

(2) Well-defined interfaces. The interfaces between adjacent (sub-)layers of the model are clearly defined. This allows more effective cooperation among the researchers who work on the different layers of trust management system and facilitates the combination of the

solutions addressing different issues of trust management. It also increases the system flexibility and prevents changes in one layer from affecting the other layers.

(3) Reducing complexity. The model facilitates modular engineering. It breaks the trust management system into smaller, simpler parts, thus aiding component development, design, and troubleshooting.

(4) Integrating policy-based and reputation-based trust. There exist two main approaches to trust management, policy-based and reputation-based approaches[7]. The former focuses on managing and exchanging credentials and enforcing access policies, while in the latter, past interactions or performance of an entity are combined to assess its future behavior. Our model, on the other hand, merges the two approaches. This is mainly due to considering two types of evidences to be gathered in the evidence layer and passed to the upper layer. This allows both the interactions outcomes and other signs –including credentials- to be taken into account in trust estimation.

Another way to integrate the credentials with the proposed model was to consider a credential as a kind of recommendation (and its issuer as the recommender entity), and so deal with the credentials in the indirect trust layer. However, we believe that this approach is preferable only in the cases where the credential issuer can be considered as a peer entity from the source entity's point of view.

7. Evaluation of the Proposed Model

To evaluate the accuracy of the proposed layer model, we applied it among some other models to the well-known dataset of Epinions. It 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.

This dataset contains no information on confidence. Accordingly, we first used our estimation method from [14], for confidence estimation. In Epinions, each trust statement contains the IDs of trustor 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, because our approach to confidence estimation needs 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.

To evaluate and compare the accuracy of the proposed model, we used the leave-one-out technique which is a common validation method in trust research works: We found all pairs (i, j) in the trust network, which the value of direct trust between them was available, and calculated the estimated trust each node n_i has in node n_j using the proposed model, as well as the well-known models of SUNNY[26], FIRE[24], Subjective Logic[2], and Dempster-Shafer-based approach[28], independently, and considered the correlation and mean of absolute error (MAE) between direct and indirect trust as measures of the accuracy for each algorithm.

The results of experiments are shown in Table 1. As the table shows, mean of absolute error in our model is 0.042 which is less than the values in other models. On the other hand, the correlation among indirect and direct trust values has been increased to 0.87.

Table 1. Comparison of the proposed model with other models using Epinions dataset

	MAE	Correlation
FIRE	0.074	0.79
SUNNY	0.048	0.82
Subjective Logic	0.063	0.80
DS-based approach	0.105	0.71
Proposed Model	0.042	0.87

8. Conclusion and Future Work

We introduced a layer model of a confidence-aware trust management system. This model provides an abstract view of the main components of the system, their functions, and the relations among them, and hence provides several advantages, including giving a global view of the system, facilitating modular engineering, simplifying the interoperability between trust researchers, and flexibility in changing/evolution of the system.

Four opinion representations, each proposed for a different layer/sub-layers of the model, allow each of them to deal with the opinions from its own point of view.

Like the other layer models used in the computing area, e.g. network layer models, our model of a trust management system, allows different solutions and implementations for the layers. In future, we are going to propose a solution stack, i.e. solutions for different layers as well as feedback management and the cross-layer units, which are not addressed in this paper. We will also work on finding optimal values for the parameters used in the model.

References

[1] A. Das, and M. M. Islam, “SecuredTrust: A Dynamic Trust Computation Model for Secured Communication in Multi-agent Systems”, *IEEE Trans. Dependable and Secure Computing*, vol. 2, no. 2, pp. 261-274 ,2012.

[2] A. Jøsang, and S. G. Knapskog, “A Metric for Trusted Systems”, *21st Security Conference*, pp. 16-29 1998.

[3] A. Jøsang, and T. Bhuiyan, “Optimal Trust Network Analysis with Subjective Logic”, *2nd Int. Conf. on Emerging Security Information, Systems and Technologies*, pp. 179-184, 2008.

[4] A. Jøsang, C. Keser, and T. Dimitrakos, “Can We Manage Trust?”, *Third International Conference on Trust Management (iTrust’05)*, pp. 93-107, 2005.

[5] B. Khosravifar, J. Bentahar, M. Gomrokchi, and R. Alam, “CRM: An Efficient Trust and Reputation Model for Agent Computing”, *Journal of Knowledge-based Systems*, vol. 30, pp. 1-16, 2012.

[6] C. Liao, C. C. Liu, and K. Chen, "Examining the Impact of Privacy, Trust and Risk Perceptions beyond Monetary Transactions: An Integrated Model", *Journal of Electronic Commerce Research and Applications*, vol. 10, no. 6, pp. 702-716, 2011.

[7] D. Artz, and Y. Gil, "A Survey of Trust in Computer Science and the Semantic Web", *Journal of Web Semantics: Science, Services and Agents on the World Wide Web*, vol. 5, no. 2, pp. 58-71, 2007.

[8] D. H. McKnight, V. Choudhury, and C. Kacmar, "Developing and Validating Trust Measures for E-commerce: An Integrative Typology", *Journal of Information Systems Research*, vol. 13, pp. 334-359, 2002.

[9] E. Sillence, P. Briggs, L. Fishwick, and P. R. Harris, "A framework for Understanding Trust Factors in Web-based Health Advice", *Journal of Human-Computer Studies*, vol. 64, no. 8, pp. 697-713, 2006.

[10] F. Chung, A. Tsiatas, and W. Xu, "Dirichlet PageRank and Trust-based Ranking Algorithms", *Workshop on Algorithms and Models for the Web Graph (WAW'11)*, pp. 103-114, 2011.

[11] F. G. Ma´rmol, and G. M. Pe´rez, "Providing Trust in Wireless Sensor Networks using a Bio-Inspired Technique", *Journal of Telecommunication Systems*, vol. 46, no. 2, pp. 163-180, 2011.

[12] F. G. Ma´rmol, and G. M. Pe´rez, "Security Threats Scenarios in Trust and Reputation Models for Distributed Systems", *Journal of Computers &Security*, vol. 28, no. 7, pp. 545-556, 2009.

[13] H. Chen, H. Wu, X. Zhou, and C. Gao, "Agent-based Trust Model in Wireless Sensor Networks", *8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networks, and Parallel/Distributed Computing*, pp. 119-124, 2007.

[14] H. Shakeri, and A. Ghaemi-B, "A Confidence-Aware Interval-based Trust Model", *Journal of IseCure*, vol. 4, no. 2, pp. 1-15, 2013.

[15] H. Shakeri, A. Ghaemi-B, and H. Sadoghi-Y, "Computing Trust Resultant using Intervals", *8th International ISC Conference on Information Security and Cryptology (ISCISC'11)*, pp. 15-20, 2011.

[16] I. K. Laia, V. W. Tongb, and D. C. Laic, "Trust Factors Influencing the Adoption of Internet-based Interorganizational Systems", *Journal of Electronic Commerce Research and Applications*, vol. 10, no. 1, pp. 85-93, 2011.

[17] J. J. Wua, Y. H. Chenb, and Y. S. Chung, "Trust Factors Influencing Virtual Community Members: A Study of Transaction Communities", *Journal of Business Research*, vol. 63, no. 9, pp. 1025-1032, 2010.

[18] 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*, vol. 10, pp. 144-154, 2010.

[19] J. Zhang, and R. Cohen, "Trusting Advice from Other Buyers in E-market Places: the Problem of Unfair Ratings", *8th Conferencece on Electronic Commerce*, pp. 235-240, 2006.

[20] L. Yan, Y. Pan, and J. Zhang, "Trust Cluster Head Election Algorithm Based on Ant Colony Systems", *3rd International Joint Conference Computational Science and Optimization (CSO)*, pp. 419-422, 2010.

[21] M. McCord, and P. Ratnasingam, "The Impact of Trust on the Technology Acceptance Model in Business to Consumer E-commerce", *International Conference on Information Resources Management Association: Innovations through Information Technology*, pp. 921-924, 2004.

[22] O. Hasan, J. M. Pierson, and L. Brunie, "Access Control in Ubiquitous Environments Based on Subjectivity Eliminated Trust Propagation", *Conference. on Embedded and Ubiquitous Computing (EUC'08)*, pp. 603-609, 2008.

[23] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins, "Propagation of Trust and Distrust", WWW Conference, pp. 403-412, 2004.

[24] T. Huynh, N. Jennings, and N. Shadbolt, "An Integrated Trust and Reputation Model for Open Multi-agent Systems", *Journal of Autonomous Agents and Multi-Agent Systems* vol. 13, no. 2, pp.119-154, 2006.

[25] T. Qin, H. Yu,C. Leung, Z. Shen, and C. Miao, "Towards a Trust-aware Cognitive Radio Architecture", *ACM Sigmobile Mobile Computing and Communications Review*, vol. 13, no. 2, pp. 86-95, 2009.

[26] U. Kuter, and J. Golbeck, "SUNNY: A New Algorithm for Trust Inference in Social Networks using Probabilistic Confidence Models", *22nd Conference on Artificial Intelligence*, pp. 1377-1382, 2007.

[27] W. Ping, Q. Jing, and Q. Y. Hui, "A Computational Trust Model with Confidence in Unstructured P2P Systems", *Joint Conference on Pervasive Computing (JCPC'09)*, pp. 451-461, 2009.

[28] X. Qiu, L. Zhang, S. Wang, and G. Qian, "A Trust Transitivity Model Based on Dempster-Shafer Theory", *Journal of Networks*, vol. 5, no. 2, pp. 1025-1032, 2010.

[29] X. Zhang, and Q. Zhang, "Online Trust Forming Mechanism: Approaches and An Integrated Model", *7th International Conference on Electronic Commerce*, pp. 201-209, 2005.

[30] Y. Wang, and M. P. Singh, "Trust Representation and Aggregation in a Distributed Agent System", *21st Conference on Artificial Intelligence (AAAI'06)*, pp. 1425-1430, 2006.