Supporting Trust in Virtual Communities

Alfarez Abdul-Rahman
Department of Computer Science,
University College London,
Gower Street, London WC1E 6BT,
United Kingdom
F.AbdulRahman@cs.ucl.ac.uk

Stephen Hailes
Department of Computer Science,
University College London,
Gower Street, London WC1E 6BT,
United Kingdom
S.Hailes@cs.ucl.ac.uk

Abstract

At any given time, the stability of a community depends on the right balance of trust and distrust. Furthermore, we face information overload, increased uncertainty and risk taking as a prominent feature of modern living. As members of society, we cope with these complexities and uncertainties by relying trust, which is the basis of all social interactions. Although a small number of trust models have been proposed for the virtual medium, we find that they are largely impractical and artificial. In this paper we provide and discuss a trust model that is grounded in real-world social trust characteristics, and based on a reputation mechanism, or word-of-mouth. Our proposed model allows agents to decide which other agents' opinions they trust more and allows agents to progressively tune their understanding of another agent's subjective recommendations.

1. Introduction

"Trustworthiness, the capacity to commit oneself to fulfilling the legitimate expectations of others, is both the constitutive virtue of, and the key causal precondition for the existence of any society" [8]. In much of our everyday lives, trusting decisions are made, be it directly or indirectly. Take the simple example of purchasing an item from a shop. We may choose to buy a certain brand because we have found it to be trustworthy in the past or it has a reputation for being widely 'trusted'. We directly trust that the store sells genuine products and not counterfeits of the brand. During purchase, the credit card transaction goes through an electronic transaction system which the cashier trusts – if the machine rejects the card, the customer is usually the suspect, not the transaction system. There is also a general trust in the soundness of the monetary system for cash transactions to proceed. Furthermore, trust, according to Luhmann [13] is also a tool for complexity reduction. This is accomplished by having trust provide the internal security before taking an action despite uncertainty and incomplete information. Several other functions of trust are named in [18]. Some of them include trust as something essential to economy and commerce, as facilitating problem solving by encouraging information exchange and influence team members, in the absorption of knowledge, in formulating a sense of self-identity and as the basis of political soundness. Trust has a silent presence in all social interactions [18].

Social interaction itself is quickly becoming a concept that spans multiple geographical, political and cultural boundaries. Virtual communities are as real as communities that meet physically or whose members exist in near or convenient proximity. Thus, whatever role trust plays in these 'physical' communities also applies to virtual communities, as, ultimately, all virtual interactions are human bound. This is true even for artificial entities such as software agents as they are created to serve a human person and the result of their interactions are fed back to humans in one form or another. Therefore, it is vital that a satisfactory trust model is provided for virtual communities so that, among others, 1) the increasing complexity of large distributed systems such as the Internet can be managed more effectively, 2) electronic commerce can proceed smoothly and 3) artificial autonomous agents can be more robust, resilient and effective by providing them with trust reasoning capabilities.

1.1. Related Work

Most of the work concerning trust in computer science have been concentrated in the area of security. These are mainly in the form of formal logics [3, 9] to analyze cryptographic protocols for design flaws and correctness. However, they are ill suited as general models of trust as

their applications are for a specific domain and they were not designed to be automated. Furthermore, no concrete definition of trust was given – the authors assumed that the intuitive notion of trust is universal. However, this is unsatisfactory because although trust is an elusive notion that is hard to define, its lack of definition opens trust models to subjective interpretations and incompatible protocol implementations. This is also true of other proposed trust models like [1, 5, 12, 15, 14, 19] and [23].

Our aim is to provide a trust model based on the real world social properties of trust, founded on work from the social sciences. As far as we know, there is only one other such similar approach to ours; that is Marsh's trust model [14]. Although the sociological foundations of his model are strong, several shortcomings are present. Firstly, Marsh tries to incorporate all aspects of social trust and introduces a large number of variables into his model. This makes his model large and complex because trust itself is a very complex and many faceted thing. Additionally, these variables are continuous values between 0 and 1 intended to represent abstract notions such as 'risk' and 'competence'. Such representations of abstract real world concepts introduce ambiguity into the model, as the semantics of these concepts are usually hard to represent as single real numbers. Furthermore, the application of one value onto another amplifies this ambiguity.

It can be said that an effective practical trust model for the virtual environment is not yet in existence.

1.2. Goals and Approach

The goal of this work is to provide a trust model for virtual communities that 1) assists users in identifying trustworthy entities and 2) gives artificial autonomous agents the ability to reason about trust. Our trust model must be based on real world characteristics of trust. The model will also need to be simple to understand so that it is intuitive and usable. Additionally, the metrics used must be unambiguous to the user. It will also need to be simple enough to implement in the codes of artificial agents, which may be subject to strict resource constraints.

In our approach to discovering the 'real-world' characteristics of trust, we turned to the social sciences. Much work have been carried out on the subject of trust in the field of sociology, philosophy, socio-psychology and economics. Thus it provides a rich environment for us to draw notes from. We then decided to work on a trust model that is based on reputation, or *word of mouth*, as this is an important trust supporting social mechanism. Additionally, we generalised the notion of reputation so that reputational information can come from an external source or from the truster himself, through experiences with other agents. In this paper, we will use the term *agent* to refer to all active trust-reasoning entities in a virtual community, human or not.

1.3. Outline of Paper

In the following section we will outline the specific definition, typology and characteristics of trust from our review of the social science literature. In Section 3, we briefly define reputation. Section 4 contains the details of the proposed trust model with the relevant data structures and operations. We then present an example application of the model in Section 5. Finally, the conclusion is presented in Section 6.

2. Trust

Trust is a social phenomenon. As such, any artificial model of trust must be based on how trust works between people in society. To this end, we have carried out a survey of the social sciences and identified characteristics of trust that are relevant to our work. We outline them below. First, we must clarify the notion of trust.

2.1. Defining Trust

Trust is a complex notion whose study is usually narrowly scoped. This has given rise to an evident lack of coherence among researchers in the definition of trust [16]. For our purposes, however, we find it instructive to use the following definition by Gambetta [9]:

> *… trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent will perform a particular action, both before [we] can monitor such action (or independently of his capacity of ever to be able to monitor it) and in a context in which it affects [our] own action.*

Mathematical probability has certain properties that make it unsuitable as a trust metric, which will be discussed in Section 2.3. For this reason, we will take Gambetta's use of the term 'subjective probability' above only as an indication of the existence of different levels of trust, which are dependent upon the truster.

2.2. Typology

Social scientists have collectively identified three types of trust. There is *Interpersonal Trust* which is the trust one agent has in another agent directly. This trust is agent and context specific [16]. For example Alice may trust a specific agent Bob the Mechanic in the specific context of

servicing her car but not in the context of babysitting her children.

The second type, *System Trust*, or *Impersonal Trust*, refers to trust that is not based on any property or state of the trustee but rather on the perceived properties or reliance on the system or institution within which that trust exists. The monetary system is one such example.

Finally, *Dispositional Trust*, or sometimes referred to as one's 'basic trust', describes the general trusting attitude of the truster. This is "a sense of basic trust, which is a pervasive attitude toward oneself and the world" [16]. Therefore, it is independent of any party or context. Further subtypes of Dispositional Trust are defined by McKnight et al [17] – Type A concerns the truster's belief on others' benevolence and Type B is the disposition that irrespective of the potential trustee's benevolence, a more positive outcome can be persuaded by acting 'as if' we trusted her.

2.3. Trust Characteristics

Trust is not an objective property of an agent but a *subjective degree of belief* about agents [16, 18]. The degrees of belief associated with trust range from complete distrust to complete trust. There is also a situation where an agent does not have an opinion of another's trustworthiness, i.e. the agent is said to be *ignorant* of the other agent's trustworthiness.

A trusting action is taken despite *uncertainty* of outcome but in anticipation of a positive outcome [4, 2, 18]. This may draw some to conclude that trust is merely a game of chance, which is untrue. More than being a blind guess, a trusting decision is based on the truster's relevant prior *experiences* and *knowledge* [11, 12]. The experiences and knowledge forms the basis for trust in future familiar situations [13]. In this sense, trust reasoning has an inductive form, rather than deductive. Furthermore, trust is *dynamic* and *non-monotonic* – additional evidence or experience at a later time may increase or decrease our degree of trust in another agent.

It may also seem intuitive to represent degrees of trust as some probability measurement. However, the problem with this is that the probability values will be meaningless unless it is based on well-defined repeatable experiments, which is an impossibility when dealing with most everyday real-life experiences. Another problem is that probability does not take the observers into account, merely their observations. Thus, probability is inherently transitive while trust is not necessarily so [12]. If Alice trusts Bob and Bob trusts Cathy, it does not necessarily follow that Alice must trust Cathy by any degree. A formal argument for the non-transitiveness of trust is given in [6]. Luhmann, in [13], considers further problems with trust and probability, while Zadeh, in [24], discusses the unsuitability of probability theory to dealing with uncertainty.

Lastly, a trusting action may not follow the rules of rational choice theory [4, 9]. An agent may have reasons beyond the cognitive evaluation of risk and utility – a trust decision may be made "in terms of here and now" instead of pondering on future outcome [4].

3. Reputation

Since it can be beyond each individual's resources to evaluate all aspects of a given situation when making a trust decision, agents must rely on other sources of information. Indeed, if complete knowledge is possible, then trust is of no use anymore. In society, we obtain information from these 'other sources' by means of word-of-mouth, i.e. a mechanism for propagating reputation. This mechanism is also a form of social control, where the behaviour of an agent in such a system is influenced by other 'participants' acting cooperatively [20, 21]. For example, a dishonest grocery store (owner) will quickly gain a reputation for dishonesty in the surrounding neighbourhood and will in the long run be forced to close shop or improve its reputation. Additionally, a good reputation may also be used to advantage, as reputation is also considered a form of social capital, especially in commerce [7].

Thus, reputational information is important in making effective and informed trust decisions. In the words of Misztal [18], "[Reputation] helps us to manage the complexity of social life by singling out trustworthy people – in whose interest it is to meet promises". The definition of reputation that we will use in this work is as follows:

> *A reputation is an expectation about an agent's behaviour based on information about or observations of its past behaviour.*

Reputational information need not solely be the opinion of others. We also include reputational information completely based on an individual agent's own personal experiences. This allows us to generalise reputational information to combine personal opinions and opinions of others for the same reputation subject.

4. The Trust Model

We propose a trust model based on sociological characteristics of trust, as described in previous sections. In particular, our model supports the following properties of social trust, as outlined in Section 2 above:

a) Trust is context-dependent[1].

b) Supports negative and positive degrees of belief of an agent's trustworthiness, although on a short range of values (four-value scale).

c) Trust is based on prior experiences. Agents are able to identify repeated experiences with similar contexts and with the same agents.

d) Agents are able to exchange reputational information through recommendations, thus supporting a reputation mechanism to assist in trust decisions.

e) Trust is not transitive – all evaluations of recommendations take into account the source of the recommendation.

f) Trust is subjective – different observers may have different perceptions of the same agent's trustworthiness.

g) Trust is dynamic and non-monotonic – further experiences and recommendations increase or decrease the level of trust in another agent.

h) Only Interpersonal Trust is supported. At this stage, we exclude Dispositional and System Trusts.

4.1. Description of Model

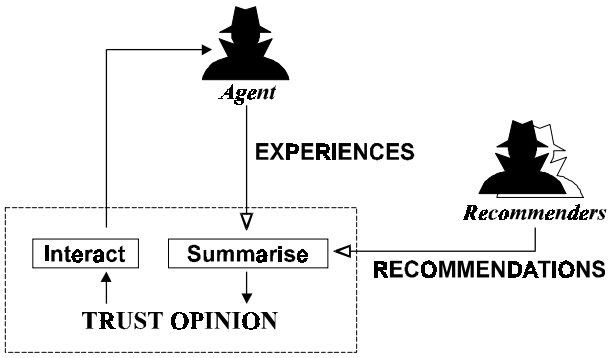

Figure 1. The Trust-Reputation Model.

Our proposed model deals exclusively with beliefs about the trustworthiness of agents based on experience and reputational information. Within the context of this paper, an *experience* is the result of a) evaluating an experience with or b) relying on a recommendation from an agent. What actions follow from an agent's trust beliefs are omitted from this paper. The reason for this is that a trusting action is based on more than just beliefs about trustworthiness. It includes, for example, aspects of risk, utility and beliefs about the motivations of other agents, which is beyond the scope of this paper. Hence, if *a* and *b* refer to agents, we will assume that inferences of the form "*a* trusts *b*" and "*a* believes *b* is trustworthy" carry the same meaning, i.e. they both state *a*'s belief about *b* rather than a trusting action.

Informally, this is a model for determining trustworthiness of agents based on the agent's collected statistics on 1) direct experiences and 2) recommendations from other agents. Agents do not maintain a database of specific trust statements in the form of "*a* trusts *b* with respect to context *c*". Instead, at any given time, the trustworthiness of a particular agent is obtained by summarising the relevant subset of recorded experiences.

4.2. Direct Trust

We represent an agent's belief in another agent's (*a*) trustworthiness within a certain context (*c*) to a certain degree (*td*) by the following:

$$t(a, c, td)$$

where $td \in \{vt, t, u, vu\}$. The semantics for *td* is given in Table 1 below. Additionally, we leave the context variable *c* open so that agents are able to define their own contexts when using this trust model.

Table 1. Trust degrees and their meanings.

Trust Degree	Meaning
vt	'Very Trustworthy'
t	'Trustworthy'
u	'Untrustworthy'
vu	'Very Untrustworthy'

4.3. Recommender Trust

The agent may also believe that another agent (*b*) is trustworthy to a certain degree (*rtd*) for giving *recommendations* about other agents with respect to a context (*c*), represented as:

$$rt(b, c, rtd)$$

A recommendation need not necessarily represent the

[1] One reviewer for this paper pointed out that our use of 'context' is similar to Tan and Thoen's use of 'categories' in their trust model [22].

belief of the recommending agent. Therefore we assume that recommenders may lie or give out contradictory recommendations to different agents. The value of *rtd* indicates the 'semantic distance' between the recommendation and *x*'s own perception of the recommended agent's trustworthiness. In other words, it is a value that is applied to 'what the recommender said' to obtain 'what I think she really means'. For example, the recommender's perception of 'very trustworthy' may only equate to what *x* perceives to be 'trustworthy', thus when a recommendation of 'very trustworthy' is made, we can apply the *rtd* value to obtain 'trustworthy'. As with direct trust, we leave the context variable *c* open.

4.4. Data Structures

An agent's opinion about another is based on their previous interactions. An agent *x* maintains this in two separate sets: the set *Q* for direct trust experiences and the set *R* for recommender trust experiences. Assume that $C = \{c_1, \ldots, c_n\}$ is the set of contexts known to an agent *x* and $A = \{a_1, \ldots, a_n\}$ is the set of agents that *x* has interacted with (either directly or as a recommender).

Further, assume that the 'grade of outcome' of an experience, *e*, is a member of the ordered set $E = \{vg, g, b, vb\}$, representing 'very good', 'good', 'bad' and 'very bad' respectively. These values correspond to the values given in Table 1.

4.5. Set *Q*

This is the set for agents that are directly trusted. For each agent *a* and context *c*, there is an associated 4-tuple $s = (s_{vg}, s_g, s_b, s_{vb})$ where s_j is an accumulator for experiences where $e = j$. Let $S = \{(s_{vg}, s_g, s_b, s_{vb})\}$. *Q* is defined as

$$Q \subseteq C \times A \times S$$

4.6. Set *R*

This is the set for trusted recommender agents. For experiences with recommender agents, the result is different. The goal is to obtain a similarity measure, referred to as the *semantic distance*, of an agent's recommendation and *x*'s perception of the outcome. As a simple example, if *a* recommends to *x* that agent *b* is 'very trustworthy' with respect to context *c*, and *x*'s evaluation of its experience with *b* is merely 'trustworthy' (a grade lower than 'very trustworthy'), then future recommendations from *a* can be adjusted accordingly. In this example, we say that *x*'s experience with *b* downgrades *a*'s recommendation by one (or that the difference is –1). The domain of possible adjustment values is given by the set $G = \{-3, -2, -1, 0, 1, 2, 3\}$.

For each agent *a* and context *c*, there are 4 sets of adjustment experiences, T_{vg}, T_g, T_b and T_{vb},. Each T_e, where $e \in E$, represents adjustments for each of *a*'s recommendations of *e*. The domain for values in T_e is the set *G*. Let $T = \{T_{vg}, T_g, T_b, T_{vb}\}$. *R* is defined as follows:

$$R \subseteq C \times A \times T$$

4.7. Evaluating Direct Trust

To determine the direct trust degree *td* in an agent *a* with respect to context *c*, or in other words, "the reputation of *a* in context *c*", first obtain the relation (*c*, *a*, *s*) from *Q*. Let $s = (s_{vg}, s_g, s_b, s_{vb})$. The value of *td* is such that *td* is the subscript or index of s_e where s_e is the largest element in *s*.

$$(1) \quad \exists td \in E \ \ \forall s_e \in s \ , (s_e = \max(s)) \Rightarrow (td = e)$$

If max(*s*) returns more than one value, then *td* is assigned an *uncertainty* value according to Table 2 below (the symbol '?' indicates 'zero or one other value').

Table 2. Uncertainty values.

e	*td*	Meaning
$vg \wedge g \wedge ?$	u^+	*Mostly good and some bad.*
$vb \wedge b \wedge ?$	u^-	*Mostly bad and some good.*
All other combinations	u^0	*Equal amount of good and bad.*

4.8. Evaluating Recommender Trust

To determine the recommender trust degree *rtd* for an agent *a* in context *c*, we first find the relation (*c*, *a*, *t*) for *a* in *R*, where $t = (T_{vg}, T_g, T_b, T_{vb})$. The value of *rtd* is obtained by taking the **mod** of the absolute values of members in the set $T^a = T_{vg} \cup T_g \cup T_b \cup T_{vb}$. This gives the distances an agent's recommendations usually are from the actual experiences from relying on its recommendations.

$$(2) \quad rtd = \text{mod}(\{\forall x \in T^a \mid |x|\})$$

4.9. Evaluating Semantic Distance

Let *sd* be a 4-tuple $(sd_{vg}, sd_g, sd_b, sd_{vb})$. To evaluate the 'semantic distance', *sd*, of a recommender *a* in context *c*, first find the relation (*c*, *a*, *t*) in *R*, where $t = (T_{vg}, T_g, T_b, T_{vb})$. Then, for each member sd_e in *sd*, assign the **mod** of

the corresponding member set T_e in t.

(3) $\forall e \in E,\ sd_e = \text{mod}(T_e)$

If T_e is multi-modal, it means that there is uncertainty in a's recommendations and further experience is required to resolve this uncertainty. In this case, we let $s_e = 0$ so that no adjustments are made when evaluating a's recommendations (shown in the next section). This allows us to take future recommendations at 'face value' and decide on the difference after the experience of relying on those uncertain recommendations.

4.10. Evaluating a Recommendation

To evaluate a recommendation of degree d from a about b's trustworthiness in context c, represented by $rec(a, b, c, rd)$, where $rd \in E$, first evaluate the semantic distance, $sd = (sd_{vg}, sd_g, sd_b, sd_{vb})$, of a for context c as shown in the previous subsection, by applying (3). Then adjust rd using the appropriate sd_{rd} value to obtain the adjusted recommended trust degree, rd^*. This is shown as

(4) $rd^* = rd \oplus sd_{rd}$

where $\oplus$ denotes the operation 'is increased by the order of'. E.g., if $rd = vg$ and $sd_{vg} = -1$ (i.e. downgrade by one) then $rd^* = vg \oplus -1 = g$.

4.11. Updating Experiences

After an experience with an agent a, the experience relation for a in Q is updated by incrementing the appropriate experience type counter. For example, if $(c, a, s = (s_{vg}, s_g, s_b, s_{vb}))$ is the appropriate relation in Q, and it was a 'good' experience (e = g), then increment s_g. Formally, given an experience of e,

(5) $s_e = s_e + 1$

Furthermore, if the experience was a result of relying on a recommendation from agent b, then we also update the experience for b in R by obtaining the appropriate relation in R for b, (c, b, t), where $t = (T_{vg}, T_g, T_b, T_{vb})$, and adding the difference between the recommended trust degree, rd, and the experience, e, to T_{rd}. The 'difference', shown by the operator $\Diamond$, is the number of levels to upgrade or downgrade rv to get e, e.g. if rd = 'very good' and e = 'good' then $e \Diamond rd = -1$, or 'downgrade by one'.

(6) $T_{rd} = T_{rd} \cup \{(e \Diamond rd)\}$

4.12. Combining Recommendations

Sometimes an agent x may encounter more than one recommender for a particular recommended agent y. To evaluate the final trust degree of y, ct_y, by combining the recommendations, we first obtain the recommender trust value, for all *known* recommenders of y (recommendations from unknown agents are discarded). If $a_1 \ldots a_n$ are the recommenders, then obtain rtd_k in each recommendation $rt(c, a_k, rtd_k)$ for $k = 1..n$. Each recommender is then assigned a weight according to their rtd_k value using Table 3 below. We then adjust the recommendations according to (4). Now, for each recommended trust degree $e \in E$, sum the weightings of the recommenders who recommended e.

Table 3. Recommender weights.

rtd_k	0	1	2	3	unknown
Weight	9	5	3	1	0

To define this formally, first, assume $a_1 \ldots a_n$ are recommenders of y, $w_1 \ldots w_n$ are their corresponding individual weightings (i.e. w_n is the weighting for a_n) and $rec(a_n, b, c, rd_n)$ is a_n's recommendation. Let L_e be the set whose members are the weights associated with recommenders who recommended e, then

(7) $\forall e \in E \ \ \forall w_i \in L_e,\ sum_e = \sum_{i=1}^{|L_e|} w_i$

The final combined trust degree, ct_y, is the sum_e with the highest value. If there are more than one largest sum_e, then ct_y is assigned an uncertainty value according to Table 2.

4.13. Bootstrapping

Although this model allows agents to learn about new recommenders and other agents completely from scratch, i.e. without any prior experience nor trusted recommenders, this is not recommended. When a new agent is created, the agent is faced with a high degree of uncertainty about other agents it may meet. This is because it will be unable to distinguish between trustworthy and untrustworthy agents. This makes the agent vulnerable to manipulation, as is any complete newcomer to any community. There is always the chance that a rogue agent may take advantage of the unwitting newcomer by pretending to offer 'assistance' for malicious hidden motives. In the real world, there are resources to guide newcomers into any field. For example,

travel guides give recommendations to travelers on aspects of a particular destination. To reduce uncertainty and risk, it is recommended that new agents are equipped with a number of 'trusted' entries in its *Q* and *R* sets so that initial interactions can be made with already trusted parties or those recommended by already trusted recommenders.

This issue is more important for artificial agents than human agents because new artificial agents are inherently less 'experienced' than human agents. An artificial agent, however, has already at least one default recommender, i.e. its human owner. Thus, there is no excuse for agents to be released into virtual communities with complete uncertainty, unless, of course, the intention is to seek out untested avenues. For such exploratory goals, it is recommended that deployed agents are robust and resilient to malicious encounters and risky environments.

5. Example Application

To illustrate use of the model, we take the example of rating recommendations for book authors. For example, we may be looking for good authors on science-fiction books. Thus, 'Science-Fiction Authors' will be our context, *c*. Assume that we have, at this time, the experience sets *Q* and *R* in the following states (r_n indicates a recommender):

R = { $(c, r_1, (\{0\}, \{\}, \{\}, \{\}))$,
$(c, r_2, (\{\}, \{\}, \{1\}, \{\}))$,
$(c, r_4, (\{\}, \{\}, \{0\}, \{\}))$ }

Q = { }

We then receive the following recommendations (recommenders r_3 and r_5 are unknown to us, as indicated by the asterisks):

Table 4. Recommendations.

Author	Recommender	Recommended Trust Degree
$author_1$	r_1	*vg*
	r_2	*b*
	$*r_3$	*g*
$author_2$	r_4	*b*
	$*r_5$	*vb*

5.1. Evaluating The Recommendations

First, obtain the recommender trust value, rtd_x, of each known recommender *x*, using (2). To illustrate this, and the remainder of this example application, we show calculations for rtd_{r2}. Results for rtd_{r1} *and* rtd_{r4} are shown in Table 5 below .

$$\begin{aligned} rtd_{r2} &= \text{mod}(\{\} \cup \{\} \cup \{1\} \cup \{\}) \\ &= \text{mod}(\{1\}) \\ &= 1 \end{aligned}$$

Then, we adjust each recommendation by first applying (3) to find their recommenders' semantic distances, i.e. find sd_b, shown here for recommender *r2*:

$$\begin{aligned} sd_b &= \text{mod}(T_b) \\ &= \text{mod}(\{1\}) \\ &= 1 \end{aligned}$$

Then adjust the recommendation by applying (4):

$$\begin{aligned} rd^* &= rd \oplus sd_b \\ &= b \oplus 1 \\ &= g \end{aligned}$$

Table 5. Result after evaluating recommendations.

Author	Recommender	rtd_x	Adjusted Recommend-ation
$author_1$	r_1	0	*vg*
	r_2	1	*g*
	$*r_3$	(ignore)	*g*
$author_2$	R_4	0	*b*
	$*r_5$	(ignore)	*vb*

Now we combine the recommendations by first assigning a weight, *w*, to each recommender using the values in Table 3, getting $w_{r1} = 9$, $w_{r2} = 5$, $w_{r3} = 0$, $w_{r4} = 9$, $w_{r5} = 0$. Finally, we sum the weights for each recommended value for each author according to (7), resulting in the table below.

Table 6. Result after combining recommendations.

Author	sum_{vg}	sum_g	sum_b	sum_{vb}

$author_1$	9	5	0	0
$author_2$	0	0	9	0

The final 'reputation' of each author is given by the level corresponding to the column of the highest sum_x value. Thus, we have the final recommended trust value, or 'reputation value', for each author as:

$author_1$ is "Very Good" (*vg*)
$author_2$ is "Good" (*g*)

5.2. Updating Experiences

We may have decided, after browsing books by the two authors, that $author_1$ is "Good" (experience $e = g$) and $author_2$ is "Bad" ($e = b$). We can then update Q using (5) and R using (6). For example, for recommender r_1, who recommended *vg* when the experience level is *g*:

$$\begin{aligned} T_{vg} &= T_{vg} \cup \{(g \lozenge vg)\} \\ &= T_{vg} \cup \{-1\} \\ &= \{0,-1\} \end{aligned}$$

We also update our experience with the books' authors in Q, using (5). For example, for $author_1$, whose book we found to be good ($e = g$):

$$\begin{aligned} s_g &= s_g + 1 \\ &= 0 + 1 \\ &= 1 \end{aligned}$$

The complete update will result in the following (new values are shown in bold):

R = { $(c, r_1, (\{0, \mathbf{-1}\}, \{\ \}, \{\ \}, \{\ \}))$,
$(c, r_2, (\{\ \}, \{\ \}, \{1, \mathbf{1}\}, \{\ \}))$),
$(c, r_4, (\{\ \}, \{\ \}, \{0, \mathbf{0}\}, \{\ \}))$),
$\mathbf{(c, r_3, (\{\ \}, \{0\}, \{\ \}, \{\ \}))}$),
$\mathbf{(c, r_5, (\{\ \}, \{\ \}, \{\ \}, \{1\}))}$) }

Q = { $\mathbf{(c, author_1, (0, 1, 0, 0)}$,
$\mathbf{(c, author_2, (0, 0, 1, 0)}$ }

Notice that we have added two new members to the set R consisting of experiences with the previously unknown recommenders. Additionally, the new authors $author_1$ and $author_2$, have been added to the direct experiences set Q. This concludes our example.

6. Conclusion

Trust forms the basis of interaction in any society, including virtual ones. In this paper we looked at the issues of trust in society and outlined a model for supporting trust in virtual communities, which is based on experience and reputation. An example application was then given for illustration. We acknowledge the ad-hoc nature of certain aspects of the model, namely the trust degrees (see Table 1) and the weightings (see Table 3). Future research will attempt to identify a more concrete representation for these metrics. Finally, it will be interesting to look into simulating artificial societies that implement the trust model presented in this paper.

7. References

[1] A. Abdul-Rahman. *The PGP Trust Model*. EDI-Forum, April 1997.

[2] A. Baier. *Trust and Antitrust*. Ethics, 96:231-260, 1985.

[3] M. Burrows, M. Abadi and R. Needham. *A Logic of Authentication*. ACM Transactions on Computer Systems, 8(1), February 1990.

[4] B. Barber. *The Logic and Limits of Trust*. New Brunswick, 1983.

[5] T. Beth, M. Borchedring and B. Klein. *Valuation of Trust in Open Networks*. In Proceedings, European Symposium on Research in Computer Security, 1994.

[6] B. Christianson and W. S. Harbison. *Why Isn't Trust Transitive?*. In Proceedings, Security Protocols International Workshop, University of Cambridge, 1996.

[7] P. Dasgupta. *Trust as A Commodity*. In, Trust: Making and Breaking Cooperative Relations, Gambetta, D (ed.). Basil Blackwell. Oxford, 1990.

[8] J. Dunn. *The Concept of Trust in the Politics of John Locke*. In, Philosophy in History, R. Rorty, J. B. Schneewind and Q. Skinner (eds.). Cambridge University Press, Cambridge, 1984.

[9] D. Gambetta. *Can We Trust Trust?*. In, Trust: Making and Breaking Cooperative Relations, Gambetta, D (ed.). Basil Blackwell. Oxford, 1990.

[9] L. Gong, R. Needham and R. Yahalom. *Reasoning about Belief in Cryptographic Protocols*. In Proceedings, IEEE Symposium on Research in Security and Privacy, Oakland, 1990.

[11] R. Hardin. *The Street Level Epistemology of Trust*. Politics and Society, 21:505-531, 1993.

[12] A. Jøsang. *The Right Type of Trust for Distributed Systems*. In Proceedings, New Security Paradigms 96 Workshop, 1996.

[13] N. Luhmann. *Trust and Power*. Wiley, Chichester, 1979.

[14] S. Marsh. *Formalising Trust as a Computational Concept*. Ph.D. Thesis, University of Stirling, 1994.

[15] U. Maurer. *Modelling a Public-Key Infrastructure*. In Proceedings, European Symposium on Research in Computer Security, 1996.

[16] D. H. McKnight, N. L. Chervany. *The Meanings of Trust*. Technical Report 94-04, Carlson School of Management, University of Minnesota, 1996.

[17] D. H. McKnight, L. L. Cummings and N. L. Chervany. *Trust Formation in New Organisational Relationships*. In Proceedings, Information and Decision Sciences Workshop, University of Minnesota, 1995.

[18] B. Misztal. *Trust in Modern Societies*. Polity Press, Cambridge MA, 1996.

[19] P. V. Rangan. *An Axiomatic Basis of Trust in Distributed Systems*. In Proceedings, IEEE Symposium on Research in Security and Privacy, Oakland, 1988.

[20] L. Rasmusson. *Socially Controlled Global Agent Systems*. Master's Thesis, Swedish Institute of Computer Science, 1996.

[21] L. Rasmusson and S. Jansson. *Simulated Social control for Secure Internet Commerce (position paper)*. In Proceedings, New Security Paradigms Workshop, Lake Arrowhead, 1996.

[22] Y.-H. Tan and W. Thoen. *Towards a Generic Model of Trust for Electronic Commerce.* In Proceedings, 12th International Bled Electronic Commerce Conference, Bled Slovenia, 1999.

[23] R. Yahalom, B. Klein, T. Beth. *Trust Relationships in Secure Systems - A Distributed Authentication Perspective*. In Proceedings, IEEE Symposium on Research in Security and Privacy, Oakland, 1993.

[24] L. Zadeh. *Is Probability Theory Sufficient for Dealing with Uncertainty in AI: A Negative View.* In Uncertainty in Artificial Intelligence, L. N. Kanal and J. F. Lemmer (eds.). Elsevier Science B. V. (North-Holland), 1986.