Tutorial

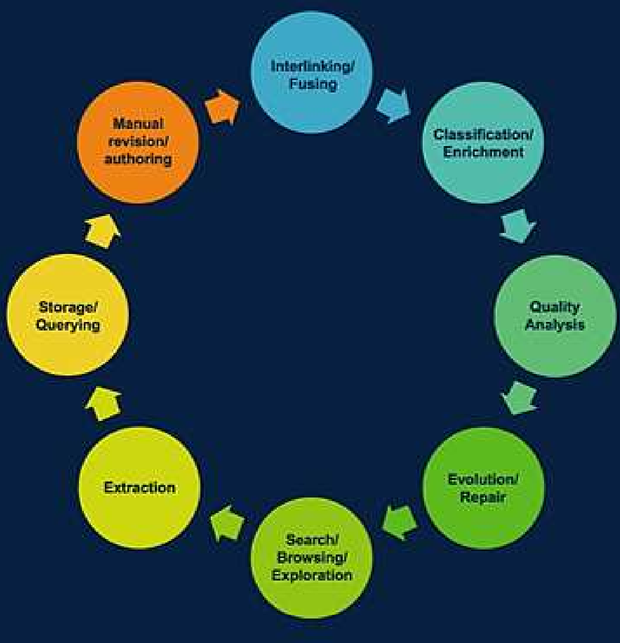
LNCS 6848

Axel Polleres Claudia d'Amato
Marcelo Arenas Siegfried Handschuh
Paula Kroner Sascha Ossowski
Peter Patel-Schneider (Eds.)

Reasoning Web

Semantic Technologies for the Web of Data

7th International Summer School 2011
Galway, Ireland, August 2011
Tutorial Lectures



Springer

Trust management methodologies for the Web

Denis Trček
Faculty of Computer and Information Science, University of Ljubljana,
Tržaška c. 25, 1000 Ljubljana, Slovenia / EU
denis.trcek@fri.uni-lj.si

Abstract. Trust and its support with appropriate trust management methodologies and technologies is becoming one crucial element for wider acceptance of web services. In the computing society trust and related issues were addressed already in the nineties of the former century, but the approaches from that period were about security, more precisely security services and security mechanisms. These approaches were followed by more advanced ones, where the first branch was based on Bayesian statistics, the second branch was based on Dempster-Shafer theory of evidence and its successors, most notably subjective logic, and the third branch originated from game theory. It is, however, important to note that at the core of trust there are cognition, assessment processes, and they are governed by various factors. Consequently, trust management methodologies should take these factors, which may ne rational, irrational, contextual, etc., into account. This research contribution will therefore provide an extensive overview of existing methodologies in the computer sciences field, followed by their evaluation in terms of their advantages and disadvantages. Further, some latest experimental results will be given that identify and evaluate some of those most important factors mentioned above. Finally, we will present a new trust management methodology called Qualitative Assessment Dynamics, QAD (aka Qualitative Algebra) that complements existing methodologies mentioned above, and that is aligned with the results of the latest experimental findings.

Keywords: web technologies, ergonomic methodologies, trust, trust management, qualitative assessment dynamics, and simulation.

1 Introduction

Before focusing on current situation in the area of computerized trust management research, it is very instructive to have a look at trust through the main epochs of development of distributed computing (web computing is certainly a kind of distributed computing).

In the mid-nineties e-business emerged and it changed the landscape of business processes significantly. In this context trusting distributed computing was (and still is) mainly about security of businesses (prevention of financial loss).

Nowadays, the Internet (as the most prominent implementation of distributed computing paradigm) is mainly entering our private domain, so trusting distributed web computing is largely related to users' personal integrity and privacy.

In the near future, web computing will intensively integrate sensor networks with the Internet, and trusting such sensor networks extended internet will add mainly questions of safety.

Now focusing on trust, the following early methodologies and solutions should be mentioned that are in fact about security (security services) and not about the core of trust. Certainly, trust can be influenced by security, but there exist important distinctions between these two terms. So the early trust related solutions are the following ones:

- Trusted Computer System Evaluation Criteria, known as the Orange Book - this standard was published by the US Department of Defense in 1985. Although it was originally intended for military systems, it became accepted for security classifications in the computer industry. And, as stated, although it was said to be about trusted computer systems, it was actually about their security.
- Platform for Internet Content Selection (PICS), which was another standard that was about access control, more precisely, web-sites filtering [1].
- PolicyMaker, which was a solution aimed at addressing trust management problems in distributed services environments. By deploying digital certificates, PolicyMaker bounded access rights to the owner of a public key. In turn, owner's identity was tied to this key by means of a certificate. Clearly, this was a PKI based trust enabling implementation [2].
- Trust Establishment Module, which was based on a dedicated language and implemented in Java. It was similar to PolicyMaker and enabled trusting relationships between unknown entities by deploying public key certificates (so this was another PKI deploying implementation) [3].

Many other early approaches are described in detail in a survey by Grandison and Sloman [4], and the reader is referred to it for additional details.

As to more contemporary and current methodologies that are used for trust management in information systems (ISs), and web environments in general, the following solutions should be considered. The simplest ones, like eBay's system, should be mentioned first. eBay's (reputation) system sums positive scores about an entity as well as negative ones, and the difference of these two results presents reputation of a particular entity. Similar approach, but a slightly more sophisticated one, and also deployed by Amazon, uses averaging, so the final score is the average of all ratings.

These two basic trust management related approaches are now being upgraded by various new, more sophisticated methodologies. This is not to say that they useless – on the contrary. They certainly have their merit, but they are essentially reputation systems. This is an important distinction, and the reasons will become clear through the presentation of current trust management methodologies in the next section.

2 Some Most Important Methodologies

One of the basic research streams for trust management in web environments is based on Bayesian statistics. This stream starts with the Bayes theorem, which states that the posterior probability of a hypothesis *H* after observing datum *D* is given by

$$p(H|D) = p(D|H) * \frac{p(H)}{p(D)}, \quad \textbf{(1)}$$

where $p(H)$ is the prior probability of *H* before *D* is observed, $p(D|H)$ is the probability that *D* will be observed when *H* is true, and $p(D)$ is the unconditional probability of *D*. Similarly, for more data, Bayes theorem can be extended (and step by step generalized) as follows:

$$p\big(H\big|(D_1, D_2)\big) = \frac{p(H, D_1, D_2)}{p(D_1, D_2)} = \cdots = p\big(D_1\big|(H, D_2)\big) * \frac{p(H|D_2)}{p(D_1|D_2)}. \quad \textbf{(2)}$$

2.1 Naïve trust management

Being the basis, Bayes theorem has served for so called naïve trust management implementations [5]. This methodology goes as follows. Suppose one is concerned with trust in competence in file providers on the web, where competences include files types, files quality, and files download speed. This problem can be represented by a Bayesian network (see Fig. 1).

With this approach every agent develops a Bayesian network for each file provider that it has interacted with. Each leaf under the root presents provider's capability in certain aspect through associated conditional probability.

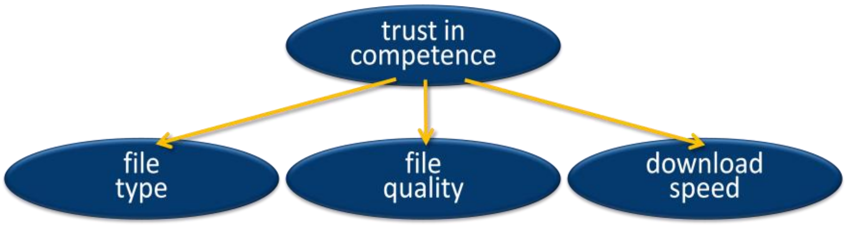


Fig. 1. Bayesian network for trust calculations related to file provider's competences.

The root of the network is assigned 1 for "satisfying", and 0 for "unsatisfying" interaction. Thus $p(T=1) = m/n$ is the percentage of satisfying, and $p(T=0) = (n\text{-}m)/n$ the percentage of unsatisfying interactions, where m stands for number of satisfying, and n for number of all interactions. The leaf nodes represent various aspects of file provider capability, so each leaf node has associated conditional probability table:

	T = 1	T = 0
music	$p(FT = \text{music} \mid T = 1)$	$p(FT = \text{music} \mid T = 0)$
movie	$p(FT = \text{movie} \mid T = 1)$	$p(FT = \text{movie} \mid T = 0)$
document	$p(FT = \text{document} \mid T = 1)$	$p(FT = \text{document} \mid T = 0)$
image	$p(FT = \text{image} \mid T = 1)$	$p(FT = \text{image} \mid T = 0)$
software	$p(FT = \text{software} \mid T = 1)$	$p(FT = \text{software} \mid T = 0)$

Table 1: The conditional probability table for a certain file provider.

In the above table $p(FT = music \mid T = 1)$ means the probability that the involved interaction is exchange of a music file given the interaction is satisfying. According to definition, it can be obtained as $p(FT = music, T = 1)/p(T = 1)$. In this equation, $p(FT = \text{music}, T = 1)$ is the probability that interactions are satisfying and that files involved are music files, while $p(T = 1)$ is the probability of satisfying interaction. $p(FT = music \mid T = 1)$ is computed as the number of satisfying interactions m_1 when files involved are music files, divided by the total number of interactions, i.e. m_1/n. Similarly, values are computed for file quality (FQ), where this quality can be "high", "medium" or "low", and for download speed (DS), which can be "fast", "medium", or "slow". This way conditional probability tables for DS and FQ are obtained.

Having these conditional probability values for nodes in Bayesian networks, an agent can calculate the probabilities about trustworthiness of a certain file provider in various aspects by using Bayes rules. For example, an agent can obtain probability that the file provider is trustworthy in providing music, $p(T = 1 \mid FT = \text{music})$, or the file provider is trustworthy in providing music files with high quality, $p(T = 1 \mid FT = \text{music}, FQ = \text{high})$. Agents update their corresponding Bayesian nets after each interaction and in case of satisfaction *m* and *n* are increased, otherwise only *n* is increased.

2.2 Theory of Evidence and Josang's Logic / Algebra

Generalization of Bayes theorem leads to the Dempster – Shaffer Theory of evidence, or ToE [6]. Its starting point is a set of possible (atomic) states, called a *frame of discernment* Θ. Within Θ, exactly one state is assumed to be true at any time.

Based on Θ, *basic probability assignment*, or *BPA* (also called *belief mass*) function is defined as

$$m: 2^{\Theta} \rightarrow [0,1], \quad \textbf{(3)}$$

where $m\{\ \} = 0$, and $\sum_{A \subseteq \Theta} m(A) = 1$. A belief mass $m_{\Theta}(X)$ expresses the belief assigned to the set *X* as a whole, and does not express any belief in subsets of *X*. Now for a subset $A \subseteq \Theta$, the belief function *bel*(*A*) is defined as the sum of the beliefs committed to the possibilities in *A*.

To illustrate ToE in a simple trust related scenario, let the frame of discernment be given by $\Theta = \{T, \neg T\}$, where "*T*" *means* that the target is trustworthy, while "$\neg T$" means the target is untrustworthy. A *basic probability assignment* for the above Θ has to be such that $m(\{T\}) + m(\{\neg T\}) + m(\{T, \neg T\}) = 1$. Now for a subset $A = \{T, \neg T\} \subseteq \Theta$, the belief function *bel*(*A*) presents the sum of the beliefs committed to the possibilities in *A*: $bel(A) = m(\{T\}) + m(\{\neg T\}) + m(\{T, \neg T\})$. For example, let $m(\{T\}) = 0.7$, $m(\{\neg T\}) = 0$, and $m(\{T, \neg T\}) = 0.3$. Now if $A=\{T\}$ then $bel(\{T\}) = m(\{T\}) = 0.7$, and if $A=\{\neg T\}$ then $bel(\{\neg T\}) = m(\{\neg T\}) = 0$.

ToE serves as a basis for subjective logic and algebra, developed by Jøsang that is also often used in computational trust management solutions [7]. This algebra introduces many new operators for modeling trust like consensus and recommendation. Trust ω is represented by a triplet (*b*, *d*, *u*), where *b* stands for belief (belief function in ToE), *d* for disbelief and *u* for uncertainty, and where values *b*, *d*, *u* are obtained from the closed interval [0, 1] as follows:

$$b(x) = \sum\nolimits_{y \subseteq x} m(y), \qquad d(x) = \sum\nolimits_{x \cap y = \emptyset} m(y), \quad \textbf{(4)}$$

$$u(x) = 1 - \big(b(x) + d(x)\big), \qquad x, y \in 2^{\Theta}.$$

Belief in a state has to be interpreted as an observer's total belief that a particular state is true. Similarly, an observer's disbelief has to be interpreted as the total belief that a state is not true. Let $\Theta = \{x_1, x_2, x_3, x_4\}$ be a frame of discernment, and let the part of power set of Θ with certain assigned values m be as given in Fig. 2 (this means that all other subsets that are not presented in Fig. 2 are assigned $m = 0$):

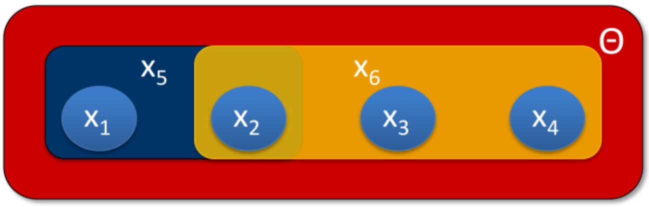


Fig. 2. An example scenario for derivation of b, d, and u.

Belief in, for example, x_5 in Fig.2, i.e. $b(x_5)$, is the sum of belief masses assigned to x_1 and x_2. Disbelief in state x_5 is the sum of the belief masses on the states x_3 and x_4 (i.e. all those that have an empty intersection with x_5). Finally, the uncertainty about x_5, i.e. $u(x_5)$, is the sum of belief masses on set x_6 and on set Θ.

As mentioned, one main contribution of subjective algebra are various trust modeling operators that preserve sound mathematical basis of ToE. Examples for conjunction, recommendation and consensus are defined as follows.

Definition 1. *Let* $\omega_p^A = \{b_p^A, d_p^A, u_p^A\}$ *and* $\omega_q^A = \{b_q^A, d_q^A, u_q^A\}$ *be agent A's opinion about two distinct binary statements p and q. Then the conjunction of and representing A's opinion about both p and q being true is defined by*

$$\omega_{p\wedge q}^A = \omega_p^A \wedge \omega_q^A = \{b_{p\wedge q}^A, d_{p\wedge q}^A, u_{p\wedge q}^A\}, \qquad \textbf{(5)}$$

where

$$b_{p\wedge q}^A = b_p^A b_q^A,$$

$$d_{p\wedge q}^A = d_p^A + d_q^A - d_p^A d_q^A, \text{ and}$$

$$u_{p\wedge q}^A = b_p^A u_q^A + u_p^A b_q^A + u_p^A u_q^A.$$

Definition 2. *Let A and B be two agents where* $\omega_B^A = \{b_B^A, d_B^A, u_B^A\}$ *is A's opinion about B's recommendations, and let p be a binary statement where* $\omega_p^B = \{b_p^B, d_p^B, u_p^B\}$

is B's opinion about p expressed in a recommendation to A. Then A's opinion about p as the result of the recommendation from B is defined by

$$\omega_p^{AB} = \omega_B^A \otimes \omega_p^B = \{b_p^{AB}, d_p^{AB}, u_p^{AB}\}, \quad \textbf{(6)}$$

where

$$b_p^{AB} = b_B^A b_p^B,$$

$$d_p^{AB} = d_B^A + d_p^B, \text{ and}$$

$$u_p^{AB} = d_B^A + u_B^A + b_B^A u_p^B.$$

Definition 3. *Let $\omega_p^A = \{b_p^A, d_p^A, u_p^A\}$ and $\omega_p^B = \{b_p^B, d_p^B, u_p^B\}$ be opinions held by agents A and B about a binary statement p. Then the consensus opinion is defined by*

$$\omega_p^{AB} = \omega_B^A \oplus \omega_p^B = \{b_p^{AB}, d_p^{AB}, u_p^{AB}\}, \quad \textbf{(7)}$$

where

$$b_p^{AB} = (b_p^A u_p^B + b_p^B u_p^A)/(u_p^A + u_p^B - u_p^A u_p^B),$$

$$d_p^{AB} = (d_p^A u_p^B + d_p^B u_p^A)/(u_p^A + u_p^B - u_p^A u_p^B), \text{ and}$$

$$b_p^{AB} = (u_p^A u_p^B)/(u_p^A + u_p^B - u_p^A u_p^B).$$

An application case of subjective algebra follows. Assume an authentication scenario where agents *B* and *C* pass the recommendation received from *D* about *E* to *A* (see Fig. 3).

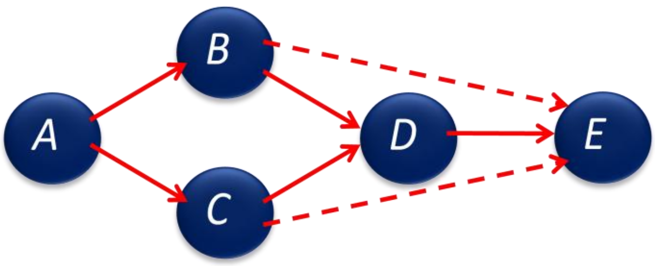


Fig. 3. PKI authentication structure example.

This situation requires the following calculations [8] (solid arrows denote first hand evidence, while dashed ones denote second hand evidence):

$$\omega^{(AB,AC)D}_{KA(k_E)} = (((\omega^A_{RT(B)} \wedge \omega^A_{KA(k_B)}) \otimes (\omega^B_{RT(D)} \wedge \omega^B_{KA(k_D)})) \oplus$$

$$((\omega^A_{RT(C)} \wedge \omega^A_{KA(k_C)}) \otimes (\omega^C_{RT(D)} \wedge \omega^C_{KA(k_D)}))) \otimes \omega^D_{KA(k_E)}.$$

In the above equation k_A denotes *A*'s public key, $\omega^A_{KA(k_B)}$ denotes *A*'s opinion about authenticity of k_B, and $\omega^A_{RT(B)}$ denotes *A*'s opinion (trust) about recommendation trustworthiness of *B*.

2.3 Yu's and Singh's ToE Based Methodology

An approach that is similar and also based on ToE is given in [9] and [10], where $\Theta = \{T, \neg T\}$ and where evidence mass function *m* is obtained as follows:

$$m(\emptyset) = 0,\; m(\{T\}) = \frac{N^+}{N},\;\; m(\{\neg T\}) = N^- / N,\; m(\Theta) = N^o / N \qquad \textbf{(8)}$$

In the above equations *N* stands for total interactions, of which N^+ denotes positive interactions, N^-negative interactions, and N°"inappreciable" interactions. This enables derivation of *bel* function (mappings) as *bel*($\{T\}$ and *bel*($\{\neg T\}$). An entity decides to trust another entity iff *bel*($\{T\}$) - *bel*($\{\neg T\}$) $\geq \rho$, where ρ is its referred to as cautiousness level.

2.4 Game Theoretic Methodologies for Trust Management

Another stream of approaches is based on game theory [11], [12]. In this theory a game consists of a set of players, a set of actions that are realizations of certain strategies available to the players, and a set of payoffs for each strategy.

One key concept in game theory is Naish equilibrium, NE. NE is important, because it represents action(s) that no other agent would prefer to deviate from, assuming that other agents also stick to it. For example, Alice and Bob are in NE if Alice makes her best decision she can while taking into account Bob's decision, and Bob makes his best decision while taking into account Alice's decision. To illustrate the central idea of game theory, the well-known prisoner's dilemma is presented in Fig. 4.

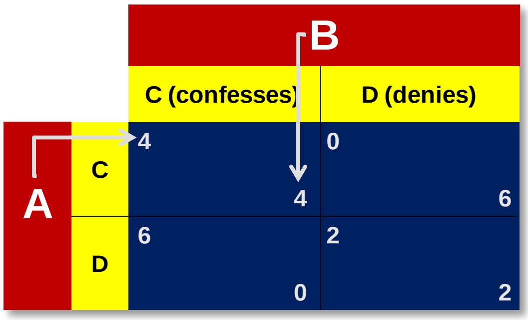


Fig. 4. The prisoners' dilemma game (C stands for confesses, D for denies).

In prisoner's dilemma two suspects are caught and offered the following choices: If they both confess the crime, they both get sentenced for four years (see the upper left dark quadrant in Fig. 4). If they deny it, both are sentenced for two years (see the lower right dark quadrant in Fig. 4). However, if one confesses while the other one not, the latter suspect gets six years of prison, while the confessing one is free (see the upper right dark quadrant and lower left quadrant in Fig. 4). This scenario clearly shows that if suspects rationally follow maximization of their self-interests they are worse off as if they were in case of cooperation (i.e., not confessing the crime and therefore not betraying the other suspect).

The formal definition of NE is as follows [11], [12]: Let N be the set of players in the game, A the set of strategy profiles, A_i the set of strategies available to player i, and u_i player i's utility function. Then a profile $a \in A$ is a Nash equilibrium (NE) if

$$\forall i \in N: a_i \in br_i(a_{-i}), \qquad \textbf{(9)}$$

where $br_i(a_{-i})$ for $i \in N, a_{-i} \in A_{-i}$ denotes the set of best responses of i to a_{-i}:

$$\underset{a_i \in A_i}{\arg\max} \{u_i(a_i, a_{-i})\}.$$

Now looking at the above game theoretic approach through trust perspective, one can observe that it is actually addressing recommendations and not trust. Therefore such approaches are about recommendation, and not trust management systems. In [13] authors present such solution, called axiomatic approach, where they study properties (termed axioms) that characterize particular aggregation rules, and analyze whether particular desired properties can be simultaneously satisfied. This axiomatic approach is tailored to personalized ranking systems with the following four basic axioms:

1. An agent would be ranked at the top of his own personalized rank.

2. An agent preferred by more highly trusted agents, should be ranked higher than an agent preferred by less trusted agents.
3. Under the perspective of any agent, the relative ranking of two other agents would depend only on the pair wise comparisons between the rank of the agents that prefer them.
4. An agent cannot gain trust by any agent's perspective by manipulating its reported trust preference.

The settings, within which the personalized ranking systems are searched for, are the domains of graphs and linear orderings. More precisely, these two definitions are the central ones for personalized ranking systems:

Definition 4. *Let A be some set. A relation* $R \subseteq A \times A$ *is called an ordering on A if it is reflexive, transitive, and complete. Let* $L(A)$ *denote the set of orderings on A.*

Definition 5. *Let* $\mathbb{G}_V^s$ *be the set of all directed graphs* $G = (V, E)$ *such that for every vertex* $v \in V$*, there exists a directed path in E from s to v. A personalized ranking system F is a function that for every finite vertex set V and for every source* $s \in V$ *maps every graph* $G \in \mathbb{G}_V^s$ *to an ordering* $\preccurlyeq_{G,s}^F \in L(V)$.

In the above definitions, let $\preccurlyeq$ be an ordering, then $\simeq$ is the equality predicate of $\preccurlyeq$, and $\prec$ is the strict order induced by $\preccurlyeq$; formally, $a \simeq b$ if and only if $a \preccurlyeq b$ and $b \preccurlyeq a$; and $a \prec b$ if and only if $a \preccurlyeq b$ but not $b \preccurlyeq a$.

Last but not least, not all game-theory based approaches are (almost) a synonym for reputation systems. There exist game-theory based approaches that do address the core of trust, and they are typically applied in multi-agent systems or MAS. Many such examples can be found in [14].

To round up this section, let us mention that the above methodological approaches are not the only ones that are used for trust management. For more extensive overview of existing approaches with focus on web environments the reader is referred to [15] and [16].

3 An Analysis of Existing Approaches

Having provided a rather extensive overview of existing trust management methodologies that have domicile in computer sciences field, we should now analyze them through trust perspective. The common shortcomings of Bayesian statistics based approaches (naïve trust management), Theory of evidence and subjective algebra are the following ones. First, agents are not (always) rational. Second, assuming that agents are rational they may still have problems with the basic notion of probability. Third, even if they do not have problems with the basic issues related to probability, they will likely not understand sophisticated mathematics that is required for ToE and subjective algebra. And finally, is trust really perceived by agents as something that can be described with $\omega = (b, d, u)$?

As to game theoretic approaches, game theory assumes rational agents, too. Further, the second tenet of game theoretic approaches is that there exists some preference. The third tenet is transitivity of preferences. But agents are not necessarily rational, or may be rational in certain contexts, but not in other contexts, e.g. the problem of irrationality in economic contexts has already been described in some outstanding research [17]. Further, experiments that will be presented in this paper indicate that for many people (or in many contexts) trust is not transitive. Moreover, agents (people) may even not have preferences when it comes to trust. This all limits application of the game theoretic approaches. There are other interesting cognitive specifics when it comes to trust – on the basis of some preliminary tests (that are yet to be experimentally proved on a wider scale) we anticipate that in certain contexts transitive preferences may become circular.

Clearly, the above trust management methodologies have certain merit. However, there exists a need for complementary methodologies, and that is where qualitative assessment dynamics, QAD, comes in. But before proceeding further, it has probably become clear to the reader that the so far presented issues are very much related to the core question, which is: *What, actually, is trust?*

We therefore need appropriate definition of trust, which will be tight enough to enable formal treatment and consequently, appropriate support with trust management applications in computing environments. In the literature there exist many definitions of trust, but one of the most authoritative ones is in the Merriam-Webster dictionary, which states that trust is assured reliance on the character, ability, strength, or truth of someone or something. This definition, although consistent, is not appropriate for our purposes, and needs further refinement and focus on web environments. One of the best candidates for our purpose is the definition given in the first half of the nineties by D.J. Dennig: Trust is an assessment that is driven by experience, shared through a network of people interactions and continually remade each time the system is used [18]. Now we can formally define trust for supporting trust management in web environments:

Definition 6. *Trust is an assessment relation between agents A and B that can be totally trusted, partially trusted, undecided, partially distrusted, and totally distrusted; it is denoted by $\alpha_{A,B}$, which means agent's A assessment of agent B.*

4 Qualitative Assessments Dynamics - QAD

Now that we have presented trust management methodologies, which are the most important and widely cited ones in the computer sciences domain, the next basic scientific question is: "How well do these methodologies reflect reality?" Or restated: "How well are existing trust management methodologies aligned with users' behavior and mental processes when it comes to trust in computerized environments?"

To find answers to above questions we started a development of a questionnaire battery in line with methodological principles for survey research in IT area in 2005 (our earlier research results can be found in [19] and [20]). The literature about these principles of research in this field is extensive, and one good example is described in [21]. It is specifically concerned with surveys for computerized applications; it is the basis for our research methodology, which is intended to get the basic knowledge about trust phenomenon for its management in computing (web) environments. These are the related fundamental questions:

- What are the main demographics of our population / sample?
- What kind of metrics is preferred when it comes to trust – quantitative, probability related assessments, or qualitative assessments?
- What is the most appropriate number of qualitative (ordinal) descriptions for users' trust assessments?
- Do agents perceive trust as a reflexive, or symmetric, or transitive relation?
- What is the influence of a society on particular agent's trust decisions?
- How is a certain trust assessment, when set for the first time, formed?
- How frequently is trust assessment changed because of no apparent reason?
- Would users allow computers to decide on their behalf when it comes to trust, or do they want to be directly involved?

Our goal with the QAD is the following. Suppose that a complementary methodology that we are aiming at should meet the requirements and expectations of such a number of users that it would be the second player on the market. Now what does it mean to be the second player? To determine this figure, one can look at market shares of most commonly used IT solutions like operating systems, web browsers and search engines. The market shares of the first three most important players in these areas are given below (see http://marketshare.hitslink.com, data as of May 2010):

- Operating systems: 91.3% Windows, 5.26% MacOS, 1.1% Linux.
- Search engines: 84.8% Google, 6.19% Yahoo, 3.24% Bing.
- Web browsers: 59.75% Internet Explorer, 24.32% Firefox, 7.04% Chrome.

It follows that to become the second player in the field, the threshold can be set as low as approx. 6% in case of operating systems, while in case of web browsers it has to be set above approx. 25%. We will set it high enough to exceed all above thresholds - to 30%.

It is now possible to state the relevant hypotheses (H_1 – H_{11}) for computationally supported trust management methodologies and solutions (these hypotheses serve to find out if our assumptions about trust management formalism properties, operators and operands, are aligned with reality or not):

- More than 30% of users would prefer direct trust management.
- More than 30% of users would prefer qualitative assessment of trust.
- More than 30% of users have problems with conforming to the basic definition of probability when it comes to trust.
- More than 30% of users would choose five levels ordinal scale for trust assessments.
- To more than 30% of users trust is not reflexive.
- To more than 30% of users trust is not symmetric.
- To more than 30% of users trust is not transitive.
- To more than 30% of users that belong to a certain group their trust assessment may generally differ from the (aggregated) assessment of the group.
- More than 30% of users may occasionally change trust assessment on a non-identifiable basis.
- To more than 30% of users that assess a certain group as a whole equals to their assessment about the majority of the members of this group.
- In more than 30% of users trust may be initialized on a non-identifiable factors basis.

Our research aimed at confirming / refuting the above hypotheses has an extensive history of almost six years. In order to make a long story short, the latest results will be briefly given. The last experiment took place in May 2010 over the web to a sample of B.Sc. students' population of computer and information sciences at FAMNIT, University of Primorska. Invitation e-mails were sent through e-mail to all 109 B.Sc. students, and the response rate was 24.1 %. Due to the conditions (anonymous participation, no benefits of whatever kind were offered, etc.) we can assume negligible response and non-response bias. Therefore we treated respondents as a random sample of the above population.

After getting and analyzing the results, we were able to confirm all hypotheses for this population, except hypothesis H3 that had to be refuted. The results are as follows (confidence interval is set to 95%, i.e. $Z = 1.96$): $H1 = 0.77 \pm 0.16$, $H2 = 0.81 \pm 0.15$, H3

= 0.42±0.19, H4 = 0.62±0.19, H5 = 0.69±0.18, H6 = 0.54±0.19, H7 = 0.69±0.18, H8 = 0.73±0.17, H9 = 0.62±0.19, H10 = 0.54±0.19, H11 = 0.58±0.19.

Taking the experimental results into account, we have developed QAD. It is aligned with THE observation that significant number of users prefers direct interaction with trust management system. Further, users prefer support of qualitative assessments on an ordinal scale, where this ordinal scale has five (descriptive, qualitative) levels. In addition, users do not perceive trust as being reflexive, symmetric, or transitive relation. Also the existence of preferences should not be assumed at all. Further, trust is driven by the community assessments, and agents choose initial trust assessments randomly (the same often holds true for already assigned trust values).

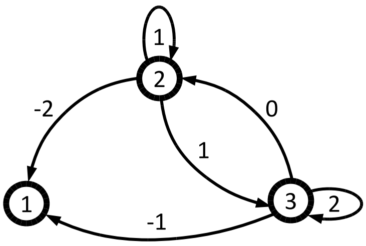
Definition 7. *Propagated trust in agents comunities is given by a trust matrix* **A***, where elements* $\alpha_{i,j}$ *denote assessment (trust relations) of i-th agent towards j-th agent, and where their values are taken from the set* $\Lambda = \{2, 1, 0, -1, -2, –\}$. *These values denote trusted, partially trusted, undecided, partially distrusted and distrusted relationships. The last symbol, "–", denotes an undefined relation, meaning that an agent is either not aware of existence of another agent, or does not want to disclose its trust.*

A general form of trust matrix **A** of a certain society with *n* agents is defined as follows:

$$A = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \cdots & \alpha_{1,n} \\ \alpha_{2,1} & \alpha_{2,2} & \cdots & \alpha_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n,1} & \alpha_{n,2} & \cdots & \alpha_{n,n} \end{bmatrix}$$

Definition 8. *In a trust matrix* **A***, columns represent society trust vector, which states society assessments about particular agent k, i.e.* $\mathbf{A}_{n,k} = (\alpha_{1,k}, \alpha_{2,k}, ..., \alpha_{n,k})$, *while rows represent agent's k trust vector, i.e.* $\mathbf{A}_{k,n} = (\alpha_{k,1}, \alpha_{k,2}, ..., \alpha_{k,n})$, *where* $k = 1, 2, \ldots, n$. *Further, excluding undefined relations from trust vector results in a society assessment sub-vector, denoted by* $\underline{\mathbf{A}}_{n1,k} = (\alpha_{1,k}, \alpha_{2,k}, ..., \alpha_{n1,k})$, *where index "*$n_1$*" denotes number of non-undefined values in a society trust vector.*

Based on the above definitions, it is possible to present an example society with trust relations, qualitative weights and corresponding matrix:



$$\begin{bmatrix} - & - & - \\ -2 & 1 & 1 \\ -1 & 0 & 2 \end{bmatrix}$$

Fig. 5. An example society graph and corresponding matrix.

Definition 9. *QAD operators belong to the set* $\Psi = \{\Uparrow, \Downarrow, \uparrow, \downarrow, \rightsquigarrow, \leftrightarrow, \odot, \updownarrow\}$, *where the symbols denote extreme optimistic assessment, extreme pessimistic assessment, moderate optimistic assessment, moderate pessimistic assessment, centralistic consensus seeker assessment, non-centralistic consensus-seeker assessment, self-confident assessment and assessment-hoping. These operators are functions* $f_j \in \Psi$, *such that* $f_j\colon \mathbf{A}_{n,i} = (\alpha_{1,i}^-, \alpha_{2,i}^-, \alpha_{3,i}^-, \dots, \alpha_{j,i}^-, \dots, \alpha_{n,i}^-) \to \alpha_{j,i}^+$, $j = 1, 2, \dots, n$, *where "j" denotes the j-th agent, superscript "-" denotes pre-operation value, superscript "+" post-operation value, and where mappings for particular operators are defined as follows:*

a) $\boldsymbol{\alpha_{j,i}^- \neq -}$**:**

- $\Uparrow_j$: $\quad max(\alpha_{1,i}^-, \alpha_{2,i}^-, \alpha_{3,i}^-, \dots, \alpha_{j,i}^-, \dots, \alpha_{n,i}^-) \to \alpha_{j,i}^+ \qquad i = 1,2,\dots,n$
- $\Downarrow_j$: $\quad min(\alpha_{1,i}^-, \alpha_{2,i}^-, \alpha_{3,i}^-, \dots, \alpha_{j,i}^-, \dots, \alpha_{n,i}^-) \to \alpha_{j,i}^+ \qquad i = 1,2,\dots,n$
- $\uparrow_j$: $$\begin{cases} \alpha_{j,i}^- \to \alpha_{j,i}^+ & if\ \dfrac{1}{n_1}\sum_{i=1}^{n_1} \alpha_{i,k}^- \le \alpha_{j,i}^- \\ \lfloor \alpha_{j,i}^- + 1 \rfloor \to \alpha_{j,i}^+ & otherwise \end{cases}$$
- $\downarrow_j$: $$\begin{cases} \alpha_{j,i}^- \to \alpha_{j,i}^+ & if\ \dfrac{1}{n_1}\sum_{i=1}^{n_1} \alpha_{i,k}^- \ge \alpha_{j,i}^- \\ \lceil \alpha_{j,i}^- - 1 \rceil \to \alpha_{j,i}^+ & otherwise \end{cases}$$
- $\rightsquigarrow_j$: $$\begin{cases} \left\lceil \dfrac{1}{n_1}\sum_{i=1}^{n_1} \alpha_{i,k}^- \right\rceil \to \alpha_{j,i}^+ & if\ \dfrac{1}{n_1}\sum_{i=1}^{n_1} \alpha_{i,k}^- < 0 \\ \left\lfloor \dfrac{1}{n_1}\sum_{i=1}^{n_1} \alpha_{i,k}^- \right\rfloor \to \alpha_{j,i}^+ & otherwise \end{cases}$$

- $\leftrightarrow_j$: $\begin{cases} \left\lfloor \frac{1}{n_1} \sum_{i=1}^{n_1} \alpha_{i,k}^- \right\rfloor \rightarrow \alpha_{j,i}^+ & if \ \frac{1}{n_1} \sum_{i=1}^{n_1} \alpha_{i,k}^- > 0 \\ \left\lceil \frac{1}{n_1} \sum_{i=1}^{n_1} \alpha_{i,k}^- \right\rceil \rightarrow \alpha_{j,i}^+ & otherwise \end{cases}$
- $\odot_j$: $\alpha_{j,i}^- \rightarrow \alpha_{j,i}^+ \qquad i = 1,2,\ldots,n$
- $\updownarrow_j$: $rand(-2,-1,0,1,2) \rightarrow \alpha_{j,i}^+ \qquad i = 1,2,\ldots,n$

b) $\boldsymbol{\alpha_{j,i}^- = -}$**:**

$$- \rightarrow \alpha_{j,i}^+ \qquad i = 1,2,\ldots,n$$

5 Analyzing Agents Behavior with QAD

A demonstration of the presented apparatus follows. Suppose we want to analyze behavior of a society that can be considered as one typical example society. It consists of 100 agents, where all agents are initially undecided about one another. Further, 90% of them are initially governed by extreme optimistic operator, while 10% are governed by extreme pessimistic operator. Now in each step 10% of population randomly changes its operator (all possible values for newly assigned random assessments and operators are equally likely). Running 30 simulation runs on this society, each of them taking 45 steps, the following histogram, presented in Fig. 7, has been obtained.

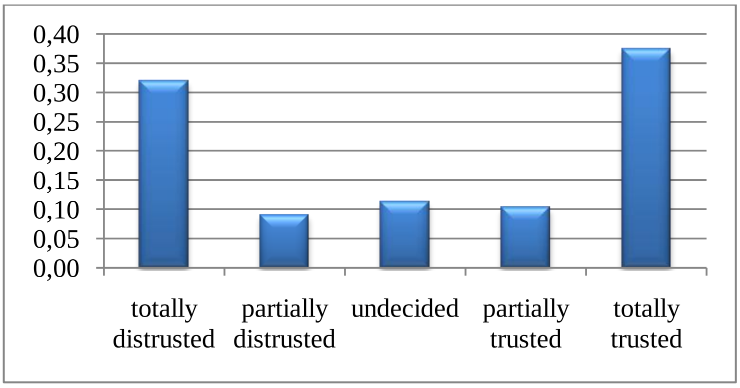


Fig. 6. Simulation results – histogram of trust values.

It follows that in such community of agents, under given conditions, the resulting distribution is (almost) bimodal. More precisely, 32% of agents become totally distrusted, and 37% of them become totally trusted. Further, 9% becomes partially distrusted, and 10% partially trusted, while for 11% of agents' population other agents remain undecided.

This is a very interesting result. Despite the fact that initially everyone was undecided about others (assuming the distribution of operators and random changes during the simulation), clear assessment patterns emerge. Further, these patterns seem to tend towards extreme assessments, so a notable polarization within the society becomes visible.

6 Conclusions

Trust has been an important topic for quite a long time in social sciences area. However, with web expansion, and e-media solutions in general, our lives have become more and more dependent on IT. This has triggered computer and information sciences researchers to start investigating intensively this area as well. This research has been further stimulated even by high ranking politicians like EU Commissioner V. Reding claiming that lack of trust is critical for wider acceptance of e-solutions, which in turn are critical for economic prosperity of the EU [22].

Certainly, the research in this area is important, not only for the web environments, because it has visible wider implications. So we anticipate that in the near future this research will be even more intensive, while at the same time the trust management infrastructure will have to be developed [23] in order to support those trust management methodologies that users will accept as the most appropriate one(s). Based on our research and experimental findings we believe that one of them may be, at least partially, Qualitative Assessment Dynamics.

Last but not least, it is worth to mention that QAD nicely complements other research efforts in this area [24]. It seems that there will not exist "one-size fits all" trust management solution when it comes to trust in web environments. Therefore some of them will be most appropriate for one kind of uses, some of them for another kind of uses. Moreover, it may even be the case that certain combinations of these methodologies may turn out to be most useful for certain practical uses and applications.

7 References

[1] Miller, J., Resnick, P., Singer, D., PICS Rating Services and Rating Systems, W3C, 1996, http://www.w3c.org/TR/REC-PICS-services.

[2] Blaze, M., Feigenbaum, J., Lacy, J., Decentralized Trust Management, Proceedings of the '96 IEEE Symposium on Security and Privacy, Oakland, pp. 164-173, 1996.

[3] Herzberg, A. et al., Access Control Meets Public Key Infrastructure, Proc. of the IEEE Conf. on Security and Privacy, Oakland, pp. 2-14, 2000.

[4] Grandison T., Sloman M., A survey of trust in internet applications, *IEEE Communications Surveys*, Vol. 3, No. 4, pp. 2–13, IEEE Society Press, 2000.

[5] Wang Y., Vassileva J., Trust and Reputation Model in Peer-to-Peer Networks, Proc. Of the 3rd Int. Conference on Peer-to-Peer Computing (P2P'03), pp. 150, Linkoping, 2003.

[6] Shafer G., *A Mathematical Theory of Evidence*, Princeton University Press, Princeton, 1976.

[7] Jøsang A., A logic for uncertain probabilities, Int. Journal of Uncertainty, *Fuzziness and Knowledge-Based Systems*, Vol. 9, No. 3, pp. 279-311, World Scientific, 2001.

[8] Jøsang A., An Algebra for Assessing Trust in Certification Chanis, *Proceedings of the Network and Distributed Systems Security Symposium, NDSS '99,* The Interent Society, San Diego, pp. 618-644, 1999.

[9] Yu B., Singh M.P., Distributed Reputation Management for e-Commerce, Proc. of the 1st AA-MAS Conference, pp. ?-?, Bologna, 2002.

[10] Paul-Amaury M., Morge M., Toni F., Combining statistics and arguments to compute trust, Proc. of the 9th Int. Conf. on Autonomous Agents and Multiagent Systems (AA-MAS), pp. 209-216, Toronto, 2010.

[11] Tennenholtz M., Game-Theoretic Recommendations: Some Progress in an Uphill Battle, Proc. of AAMAS 2008, pp. 10 -16, Estoril, 2008.

[12] Harish M., Anandevelu N., Anbalagan N., Mahalakshmi G.S., Geetha T.V., Design and Analysis of a Game Theoretic Model for P2P Trust Management, Distributed Computing and Internet Technology, pp. 110 - 115, Springer, Heidelberg, 2007.

[13] Altman A. and Tennenholtz M., An axiomatic approach to personalized ranking systems, Proceedings of the 20.th international joint conference on Artificial intelligence (IJCAI'07), Morgan & Kaufmann, San Francisco, 2007, pp. 1187-1192.

[14] Sabater J. and Sierra C., Review on Computational Trust and Reputation Models, Artificial Intelligence Review, Vol. 24, No. 1, pp. 33-60, Springer, 2005.

[15] Golbeck J., Trust on the World Wide Web: A survey, Foundation and Trends in Web Science, Vol. 1, No. 2, pp. 131-197, Now Publishers, 2006.

[16] Artz D., Gil Y., A survey of trust in computer science and the Semantic Web, Software Engineering and the Semantic Web, Vol. 5, No. 2, pp. 58-71, Elsevier, 2007.

[17] Kahneman D., Slovic P., A. Tversky (Eds.), *Judgment Under Uncertainty*, 22nd reprint, Cambridge University Press, Cambridge, 2006.

[18] D. Denning, A new Paradigm for trusted systems, Proc. of ACM SIGSAC New Security Paradigms Workshop, ACM, pp. 36–41, New York, 1993.

[19] Trček D., A formal apparatus for modeling trust in computing environments, *Mathematical and Computer Modeling*, Vol. 49, No. 1-2, pp. 226–233, Elsevier, 2009.

[20] Trček D., Ergonomic trust management in pervasive computing environments - qualitative assessment dynamics, Proceedings of the ICPCA '10, IEEE Press, Maribor, 2010, pp. 1-7.

[21] Pfleeger S.L., Kitchenham B.A., Principles of Survey Research, Parts 1-6, ACM Software Engineering Notes, Vol. 26-28, ACM, 2001-2003.

[22] Reding V., The need for a new impetus to the European ICT R & I Agenda, Int. High Level Research Seminar on "Trust in the Net", Vienna, 2006.

[23] Kovač D., Trček D., Qualitative trust modeling in SOA, *Journal of Systems Architecture*, Volume 55, Issue 4, pp. 255-263, Elsevier North-Holland, 2009.

[24] Grabner-Kraeuter S., Kaluscha E. A., Empirical Research in on-line trust: a review and critical assessment, International Journal of Human Computer Studies, Vol. 2003, No. 58, pp. 783–812, Elsevier, 2003.

8 Acknowledgement

The Slovene Research Agency has financed this research through research program P2-0359. Special thanks go also to both reviewers for their helpful comments and suggestions.