Qualitative Assessment Dynamics For Trust Management in e-Business Environments

Denis Trček
Faculty of Computer and Information Science
University of Ljubljana
Tržaška cesta 25, 1000 Ljubljana, Slovenia - EU
Faculty of Mathematics, Natural Sciences and Inf. Technologies
University of Primorska
Glagoljaška 4, 6000 Koper, Slovenia - EU
denis.trcek@fri.uni-lj.si

Eva Zupančič
Faculty of Computer and Information Science
University of Ljubljana
Tržaška cesta 25, 1000 Ljubljana, Slovenia - EU
eva.zupancic@fri.uni-lj.si

***Abstract*—Trust is a core issue when it comes to acceptance of contemporary e-services. It was first addressed almost thirty years ago in Trusted Computer System Evaluation Criteria standard by the US DoD. But this and other proposed approaches of that period were actually addressing security. Roughly some ten years ago, methodologies followed that addressed trust phenomenon at its core, and they were based on Bayesian statistics and its derivatives, while some approaches were based on game theory. However, trust is a manifestation of judgment and reasoning processes. It has to be dealt with in accordance with this fact and adequately supported in e-environments. On the basis of the results in the field of psychology and our own research, a methodology called qualitative assessment dynamics (QAD) has been developed, which deals with so far overlooked elements of trust phenomenon. It complements existing methodologies and provides a basis for comprehensive trust management in e-environments.**

***Keywords*-distributed e-services; trust management; reasoning and judgment; modeling and simulation**

I. Introduction

Trust is an important phenomenon that forms the basis for many of our everydays decisions. Cyber space is no exception - the more sensitive an interaction in terms of security, privacy or safety is, the more trust there has to exist for an entity is to engage into an interaction. Some researchers even claim that trust is such essential resource that it is the main social virtue for the prosperity of societies [6]. Trust certainly has economic implications: In a trusted society business processes may run smoother and cheaper, because there is a reduced need for many checks (e.g., business reports), and acquisition of various means of insurance (e.g., bank guarantees, letters of credit). To ordinary users this may not appear familiar, but considering e-business environments like e-Bay, it becomes clear that trust in e-environments has significant business implications. Last but not least, the importance of trust is evident also to the highest ranking officials in the EU Commission that are stating that ”there is not yet enough trust in the Net” [19].

Before going into methodological details it is necessary to give the basic definitions first. According to the Cambridge Advanced Learner’s Dictionary, *trust is a belief or confidence in the honesty, goodness, skill or safety of a person, organization or thing*. For trust management in e-environments, this definition is not sufficient. A better definition is the one provided by Denning at the beginning of the nineties [4], when trust started to be more and more exposed in relation to security in information systems (IS). She vividly concluded that *trust is not a property of an entity or a system, but is an assessment. Such assessment is driven by experience, it is shared through a network of people interactions and it is continually remade each time the system is used*. And what is reputation? According to the Cambridge Advanced Learner’s Dictionary, *reputation is the opinion that people in general have about someone or something, or how much respect or admiration someone or something receives, based on past behaviour or character*. This enables us to treat reputation as an aggregated trust on the level of a certain society. Consequently, trust presents the basic building block, and we will concentrate on it in the rest of the paper.

The paper is structured as follows. In the second section an overview of existing methodologies for computerized trust management is given. In the third section a new, complementary methodology, called qualitative assessment dynamics (aka qualitative algebra) is presented that takes into account also research done in the field of psychology. There is a brief description of a technological solution for computerized trust management in the fourth section, while conclusions are given in the fifth section. The paper ends with the references in the last section.

II. A Brief Overview of the Field

A large number of initiatives in the field of trust management in e-environments came from the security research area. The main reason is probably that security and trust are

 ISBN:978-1-61208-114-4

closely related. These terms were used interchangeably as if they were expressing largely overlapping notions, which can be seen in early technical solutions. Although these were trust focused solutions, they were in fact security solutions. The first example is from 1996 when the World Wide Web Consortium standardized a Platform for Internet Content Selection (PICS) [13]. This technology was about access control, more precisely web-sites filtering. Web pages were rated by using defined labels and browsers could be set to exclude pages with a particular PICS rating or pages without this rating. The second example also dates back to 1996 when AT&T developed PolicyMaker, which was aimed at addressing trust management problems in network services [2]. Again, this was primarily a security solution that bounded access rights to the owner of a public key, whose identity was bound to this key through a certificate. The third example is from the year 2000, when IBM entered the area with the Trust Establishment Module [7]. This module was a Java based solution with appropriate language, similar to PolicyMaker. It enabled trusting relationships between unknown entities by using public key certificates and security policy.

At the turn of the century, EU funded projects followed that targeted trust. These attempts were already closer to addressing user behavior and the essence of trust, but many can be still characterized as largely security related technologies - some of them follow next. ITrust was a forum for cross-disciplinary investigation of the application of trust as a means of establishing security and confidence in the global computing infrastructure, where trust was recognized to be a crucial enabler for meaningful and mutually beneficial interactions [10]. TrustCOM was a framework for trust, security and contract management in dynamic virtual organizations. It was intended to be an open source reference implementation that builds on public specifications [5]. And finally INSPIRED was aimed at developing the next generation of security technologies needed for trusted access of users to e-services in a mobile or fixed environment. It was focused on smart-cards [12].

An interesting research from a non-security domain is described in the work of Cassell and Bickmore [3]. This approach addresses the essence of trust by deploying small talk to model social language and developing a collaborative relationship with users in agents based applications. Another interesting approach is taken in TRUSTe project [22] that is intended for promoting on-line business. TRUSTe services allow companies to communicate their commitment to privacy, and let consumers know which businesses they can trust. A similar approach is given in [17], where trust is supposed to be a matter of accreditation and certification of IT technology, which certainly makes sense within specific contexts.

Getting now to the theoretical basis, trust in computing environments is most often treated on the basis of Bayes theorem as the starting point. The theorem states that the posterior probability of a hypothesis H after observing datum D is given by $P(H \mid D) = P(D \mid H) * P(H)/P(D)$, where $P(H)$ is the prior probability of hypothesis H before datum D is observed, $P(D \mid H)$ is the probability that D will be observed when H is true, while $P(D)$ is the unconditional probability of datum D. This theorem has been used mainly for so called naïve trust management implementations [23].

A generalized Bayes theorem, the Dempster Shaffer theory of evidence, extends the classical concept of probability, where a probability p of stochastic event x, i.e. $p(x)$, and probability p of its complement $\overline{x}$, i.e. $p(\overline{x})$, sum up to 1. It does this by introducing uncertainty, meaning that $p(x) + p(\overline{x}) < 1$. The theory serves as a basis for subjective algebra, developed by Jøsang that is also used in computational trust management [9]. This algebra defines a set of possible states, a frame of discernment Θ. Within Θ, exactly one state is assumed to be true at any time. So if a frame of discernment is given by atomic states x_1 and x_2, and a compound state $x_3 = \{x_1, x_2\}$, which means that $\Theta = \{x_1, x_2, \{x_1, x_2\}\}$. Then, the belief mass is assigned to every state and in case of, e.g., x_3 it is interpreted as the belief that either x_1 or x_2 is true (an observer cannot determine the exact sub state that is true). Belief mass serves as a basis for belief function, which is interpreted as a total belief that a particular state is true, be it atomic or compound. This gives a possibility for rigorous formal treatment on a mathematically sound basis, where subjective algebra, in addition to traditional logical operators, introduces new operators like recommendation and consensus, and where trust is modeled with a triplet (b, d, u): b stands for belief, d for disbelief and u for uncertainty. Each of those elements obtains its values from the interval [0, 1], such that $b + d + u = 1$.

Finally, among main-stream methodologies that have been developed for computational trust management also game theoretic based ones should be mentioned - one typical representative is [1].

III. Qualitative Assessment Dynamics

The basis for methodology presented in this section is the research done in the area of psychology that provides an additional useful perspective on trust as a kind of reasoning and judgment process [18], [14], [15], and our own research [21]. Taking these works into account, the main factors that have to be considered are the following ones (for additional explanations of the above factors and their use for a formalized model that supports trust in computing environments, a reader is referred to [20]):

- Temporal dynamics - agent's relation towards the object / subject being trusted is certainly a dynamic relation that changes with time.

- Rationality and irrationality - an agent's trust can be driven by rational or irrational factors.
- Feed-back dependence - trust is not a result of an independent mind, but is influenced by environment.
- Action binding - trust can be a basis for agent's deeds.
- Trust differentiation - trust evolves into various forms because of the linguistic abilities of an entity expressing trust, or its intentions, and because of perception capabilities of a targeting entity.

The above works provide the main guidelines. However, additional reasons that suggest the need for a new, qualitative methodology, are the following (these address the shortcomings of the existing methodologies that are described in the previous section):

1) As to Bayesian statistics based methodologies, subjects have to understand basic concepts. However, many research results show that users often have problems with basic mathematical concepts like probability (see, e.g., [16]). Now even if subjects understand these basic mathematical concepts, very few of them understand advanced concepts that are required by, e.g., theory of evidence.
2) Methodologies that are based on game theory cannot be generally used for trust because of problems with preferences. In case of trust, preferences need not to exist, while in case of their existence, they are not necessarily transitive. So the two basic tenets of game theory are not fulfilled.
3) Our research indicates that users prefer qualitative expressions over quantitative ones when trust is in question. The qualitative ordinal scale is likely to consist of five ranks (qualitative descriptions) [21].

These facts call for a complementary method, which will be defined in the rest of this section.

Definition 1. *Trust is a relationship between agents A and B that can be totally trusted, partially trusted, undecided, partially distrusted, and distrusted; it is denoted by $\omega_{A,B}$, which means agent's A attitude towards agent B.*

The below figure illustrates the definition. There are four trust relationships, two of them addressing judgments of entities A and B towards themselves ($\omega_{A,A}$ and $\omega_{B,B}$), and two of them addressing judgment of one entity towards another entity ($\omega_{A,B}$ and $\omega_{B,A}$).

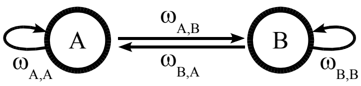

Figure 1. The definition of trust relationships

Next, the general nature of trust is that it is not reflexive (in certain contexts one may trust himself / herself, in others not), not symmetric (if agent A trusts agent B in a certain context, this gives no basis for automatic conclusion that agent B also trusts agent A), and not transitive (entity A may trust entity B, which in turn may trust entity C, but the latter may not be trusted by A).

This already suggests that trust is not an easy problem. Moreover, it can be proved that it is computationally hard problem - a proof outline follows: Suppose entity A assigns trust value for herself in a certain context, while entity B assigns another value to himself in the same context. When these entities are treated as a new compound entity AB (a team), the trust of this compound entity towards itself often differs from both trust values mentioned earlier (a typical example are sports games where an additional player in a team presents advantage for the whole team and changes judgments about its capabilities at all members of the team). The above fact implies that all relationships have to be considered among all possible entities, be it atomic or compound. As the number of compound entities can be obtained by computing the number of combinations that can be formed from the set of atomic entities, the total number of trust relationships N in a society with n atomic entities is given by the following equation:

$$N = (\sum_{m=1}^{n} \binom{n}{m})^2 \tag{1}$$

Suppose we have a society with $n = 3$ atomic entities A, B and C. This means that the number of atomic entities is three, the number of compound entities with two atomic elements is three, and the number of compound entities with three atomic elements is one. So the total number of atomic and compound entities is $k = 7$, and there are $(k-1)*k$ relationships between them, where k relationships have to be added, because trust is not reflexive. Thus the total number of trust relationships is $N = 49$.

To enable the analysis and modeling of trust dynamics in social environments trust graphs are introduced. The links of trust graphs are directed and weighted accordingly. If a link denotes trust attitude of agent A towards agent B, the link is directed from A to B. Because graphs can be equivalently presented with matrices, this second definition can be given.

Definition 2. *In a given context Γ, trust in social interactions is represented by trust matrix $\mathbf{M}_\Gamma$, where elements $\omega_{i,j}$ denote trust relationships of i-th agent towards j-th agent, and where its values taken from the set $\{1, 1/2, 0, -1/2, -1, -\}$. These values denote trusted, partially trusted, undecided, partially distrusted and distrusted relationships. The last symbol, "-", denotes an undefined relation (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 $\mathbf{\Omega}_\Gamma$ of a certain society with n agents in a given context Γ is as follows:

 ISBN:978-1-61208-114-4

$$\begin{bmatrix} \omega_{1,1} & \omega_{1,2} & \cdots & \omega_{1,n} \\ \omega_{2,1} & \omega_{2,2} & \cdots & \omega_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_{n,1} & \omega_{n,2} & \cdots & \omega_{n,n} \end{bmatrix}_{\Gamma}$$

An example of a certain society with trust relationships and qualitative weights is given in Fig. 3:

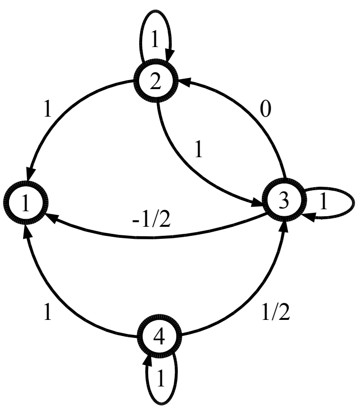

Figure 2. An example society that includes a dumb agent

The corresponding matrix is as follows:

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

Trust matrices operations differ from those in ordinary linear algebra. Rows represent certain agents trust towards other agents, while columns represent trust of community related to a particular agent (columns are referred to as trust vectors). Further, technological components or services are treated as dumb agents. They can be recognized in a trust matrix by rows that consist exclusively of ”–” values.

It is a fact that certain entity may not equally treat all judgments from various entities, therefore there has to exist a possibility for pondering values. This is achieved by introduction of a ponder matrix $\mathbf{\Pi}$:

$$\begin{bmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n,1} & p_{n,2} & \cdots & p_{n,n} \end{bmatrix}_{\Gamma}$$

Above, $p_{i,j}$ states a weight (from the interval [0,1]) that an entity i is assigning to judgments of entity j. Therefore, rows represent ponders that a certain entity is assigning to judgments of all other entities in a society. To keep things simple, this matrix will be left out the rest of the paper.

Now qualitative operators can be introduced; they are taken from the set $\{\Uparrow, \Downarrow, \leadsto, \leftrightarrow, \uparrow, \downarrow, \odot\}$, and defined in detail in table 1, and described below:

- Extreme-optimistic judgment, which results in the most positive judgment in a society; it is denoted by ”$\Uparrow$”.
- Extreme-pessimistic judgment, which outputs the most negative judgment in a society; it’s denoted by ”$\Downarrow$”.
- Centralistic consensus seeker judgment, which results in a towards zero ”rounded average”; its symbol is ”$\leadsto$”.
- Non-centralistic consensus-seeker judgment, which results in a value that is ”an average” rounded away from 0; it’s denoted by ”$\leftrightarrow$”.
- Moderate optimistic judgment, which means the expressed judgment is ”strengthened” to the next higher level, narrowing the gap towards the aggregated judgment of the rest of community if this is more optimistic than the agent’s trust is; it is denoted by ”$\uparrow$”.
- Moderate pessimistic judgment, which means the expressed judgment is weakened to the next lower level, narrowing the gap towards the aggregated judgment of the rest of community if this is more pessimistic than the agents trust is (the value changes one level downwards); it is denoted by symbol ”$\downarrow$”.
- Self-confident judgment, which preserves the same value after changes are calculated; its symbol is ”$\odot$”.

For the calculation of new trust values (and new trust matrix) the following algorithm is defined:

1) Take the first value in a trust matrix.
2) If the value is ”-”, write again ”-”, and go to step 6.
3) Calculate the average of a trust vector by excluding agents own opinion and values marked with ”-”.
4) Round the obtained average to the nearest possible judgment value from the set of judgment increments $\{1, 1/2, 0, -1/2, -1\}$.
5) Compute the result $\omega^{+}_{i,k}$ according to table 1 by treating the value from step 4 as $\omega^{-}_{j,k}$, and agents own opinion as $\omega^{-}_{i,k}$.
6) If there still exist unprocessed values, take the next value from the trust matrix and go to step 2, else stop.

Now suppose that in the example society in Fig. 3 agent 2 conforms to the optimistic operator, agent 3 to pessimistic operator, while agent 4 is a centralistic consensus seeker, the calculated simulation would be as follows:

$$\begin{matrix} \\ \Uparrow \\ \Downarrow \\ \leadsto \end{matrix} \begin{bmatrix} - & - & - & - \\ 1 & 1 & 1 & - \\ -1/2 & 0 & 1 & - \\ 1 & - & 1/2 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} - & - & - & - \\ 1 & 1 & 1 & - \\ -1/2 & 0 & 1/2 & - \\ 1/2 & - & 1/2 & 1/2 \end{bmatrix}$$

Note that matrices $\mathbf{M}_{\Gamma}$ contain non-calculated values, but only ”pure judgments” entered by entities. They constitute, so to say, raw data for our calculations that are used by our algebra to support decision making. Now some important decision making questions are as follows:

- By running the simulation on a given society, is the society likely to reach an equilibrium?
- If it does reach an equilibrium, which entities will be most likely trusted by the society, and which not?

ISBN:978-1-61208-114-4

- How long will it take for the society to reach the most likely state and what state will this be?
- On which part of the society makes most sense to put most efforts to drive the community into a desired state?

$\omega^-_{i,k}$	$\omega^-_{j,k}$	$\omega^+_{i,k}$, $\Uparrow_i$	$\omega^+_{i,k}$, $\Downarrow_i$	$\omega^+_{i,k}$, $\rightsquigarrow_i$	$\omega^+_{i,k}$, $\leftrightarrow_i$	$\omega^+_{i,k}$, $\uparrow_i$	$\omega^+_{i,k}$, $\downarrow_i$	$\omega^+_{i,k}$, $\odot_i$
-1	-1	-1	-1	-1	-1	-1	-1	-1
-1	-½	-½	-1	-½	-1	-½	-1	-1
-1	0	0	-1	-½	-½	-½	-1	-1
-1	½	½	-1	0	-½	-½	-1	-1
-1	1	1	-1	0	0	-½	-1	-1
-1	–	–1	-1	-1	-1	-1	-1	-1
-½	-1	-½	-1	-½	-1	-½	-1	-½
-½	-½	-½	-½	-½	-½	-½	-½	-½
-½	0	0	-½	0	-½	0	-½	-½
-½	½	½	-½	0	0	0	-½	-½
-½	1	1	-½	0	½	0	-½	-½
-½	–	-½	-½	-½	-½	-½	-½	-½
0	-1	0	-1	-½	-½	0	-½	0
0	-½	0	-½	0	-½	0	-½	0
0	0	0	0	0	0	0	0	0
0	½	½	0	0	½	½	0	0
0	1	1	0	½	½	½	0	0
0	–	0	0	0	0	0	0	0
½	-1	½	-1	0	-½	½	0	½
½	-½	½	-½	0	0	½	0	½
½	0	½	0	0	½	½	0	½
½	½	½	½	½	½	½	½	½
½	1	1	½	½	1	1	½	½
½	–	½	½	½	½	½	½	½
1	-1	1	-1	0	0	1	½	1
1	-½	1	-½	0	½	1	½	1
1	0	1	0	½	½	1	½	1
1	½	1	½	½	1	1	½	1
1	1	1	1	1	1	1	1	1
1	–	1	1	1	1	1	1	1
–	*	–	–	–	–	–	–	–

Figure 3. The definition table for qualitative operators ($*$ means any value)

GUI of trustGuard component that is used for QAD simulations is given in Fig. 4. The parameters were set as follows: The complete society consisted of ten agents, of which 40% behaved according to optimistic operator, 20% according to pessimistic operator, and there were 20% opponents and 20% centralists. Further, the initial distribution of trust values in the trust matrix was 20% of values denoted by 1, 20% denoted by $1/2$, 20% denoted by 0, 20% denoted by $-1/2$, and 20% denoted by -1 (there was no dumb agent). In addition, 30% of agents were allowed to randomly change their operators, and there were 5 simulation steps between these random changes. After running the situation for a sufficiently rong time (for approx. 970 steps), we reach an equilibrium, where 10% of values in the trust matrix 0 (i.e. undecided), while 90% of values were -0.5 (partially distrusted). Finally, an agent with a fat line around it is partially distrusted by the society in the end.

Despite the fact that more detailed discussion of the simulation processes exceeds the scope of the paper, an experienced reader can see that this component enables sound simulations by providing, e.g., expected values for variables in question, their distribution, etc. To conclude this section - it clearly follows that we are dealing with a non-linear dynamic system. Therefore analytic solutions will be mere exceptions and we will have to rely on simulations (to search for various heuristics and solutions for typical, reference scenarios, etc.). Despite this, various interesting theoretical questions can be addressed [21]).

IV. Trust Management Implementation

Our solution for trust management is called trustGuard. It consists of two basic building blocks: the distributed database where trust values (matrices) are stored, and the user interface that accesses this database, performs insertion and retrieval of these values, and does QAD calculations. The distributed database is implemented on SOA standards, so user interface interacts with these databases through SOAP protocol. For this to happen, the following two primitives are needed. The first one is *trustQuery*, and the second one is *trustReply*. These primitives are defined with XML schema. But for clarity and conciseness, XML DTD is chosen to present the syntax of *trustReply* primitive:

```
<!ELEMENT   trustResponse (timeStamp, trustMatrix,
            function?, extension?) >
<!ELEMENT   timeStamp (#PCDATA) >
<!ATTLIST   timeStamp zulu
            CDATA #REQUIRED >
<!ELEMENT   trustMatrix (omega+) >
<!ELEMENT   omega (id1, id2, trustAssessment) >
<!ELEMENT   id1 (#PCDATA) >
<!ATTLIST   id1 URI1
            CDATA #REQUIRED >
<!ELEMENT   id2 (#PCDATA) >
<!ATTLIST   id2 URI2
            CDATA #REQUIRED >
<!ELEMENT   trustAssessment EMPTY >
<!ATTLIST   trustAssessment
            value (−1| − 0.5|0|0.5|1|−) ” − ” >
<!ELEMENT   function (#PCDATA) >
<!ATTLIST   function OID
            CDATA #REQUIRED >
<!ELEMENT   extension (#PCDATA) >
```

The generalized time is expressed as Greenwich Mean Time (Zulu) in the form YYYYMMDDHHMMSS, while trust assessment functions are uniquely identified through OIDs [8]. The syntax of *trustQuery* is similar to the syntax of *trustReply*, except that there are no *trustMatrix* elements. The *extension* element is included and is added in both primitives for future extensions.

Current trustGuard implementation supports not only qualitative algebra, but also, e.g., Jøsang' s subjective algebra. As further implementation details exceed the scope of this paper, a reader can find more information in [11].

V. Conclusion

In the medieval era, Shakespeare advised us to love all, trust a few, and do wrong to none. Later, the famous German

 ISBN:978-1-61208-114-4

poet Goethe, with a strong sense for deep analyses claimed that as soon as one trusted himself (herself), one knew how to live. And recently, prof. H. Smead vividly noted: ”When we were young, we didn’t trust anyone over thirty. Now that we’re over thirty, we don’t trust anyone at all”.

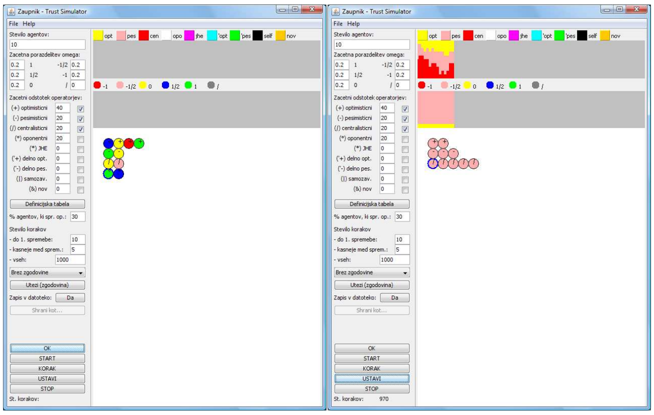

Figure 4. An example of a simulation run with the trustGuard component

It follows that trust is a sensitive and scarce resource. This especially holds true for e-business environments, where competition is only a few mouse clicks away, while the medium by its nature is not able to provide communication details that are available in face to face contacts; therefore new mechanisms have to be developed and deployed. Further, if users are to be adequately supported when trust management is an issue, the solutions have to be aligned with mental models. These issues have led to the development of qualitative algebra, and they were also the basis for theoretical views, as well as for the practical implementation.

Qualitative algebra complements existing approaches that depend on rational mechanisms like Bayesian statistics and game theory. It is based on research in the field of psychology and addresses irrational elements, feed-back dependence, and context dependence. It provides basic means also for more advanced problems through simulations like ”How can a society be guided in order to achieve (with a certain probability) a trusted atmosphere?”. Clearly, with questions like this simulation is one of the most suitable approaches, because trust related problems belong to the area of complex, non-linear dynamics. Thus computationally supported trust management is not only a must because of the nature of e-media, but because of the trust phenomenon itself.

Acknowledgment

Authors thank to Slovene Research Agency ARRS for support of this research with grants J2-9649 and P2-0359 (Pervasive computing).

References

[1] Aberer K. and Despotovic Z., *On Reputation in Game Thory - Application to Online Settings*, Working Paper, Swiss Federal Institute of Technology (EPFL), Zurich, 2004.

[2] Blaze M. and Feigenbaum J., Lacy J., Decentralized Trust Management, *Proc. of the ’96 IEEE Symposium on Security and Privacy*, Oakland, pp. 164–173, 1996.

[3] Cassel J., Bickmore T., Negotiated Collusion - Modeling Social Language and its Relationship Effects in Int. Agents, *User Model. & User-Adapted Int.*, 13(4), pp. 89–132, 2003.

[4] Denning D., A new Paradigm for Trusted Systems, *Proc. of ACM SIGSAC New Security Paradigms Workshop*, ACM, New York, pp. 36-41, 1993.

[5] Dimitrakos T., Wilson M., Ristol S., TrustCoM - A Trust and Contract Management Framework enabling Secure Collaborations in Dynamic Virtual Organisations, *ERCIM News*, 2004(59), pp. 59–60, 2004.

[6] Fukuyama F., *Trust: The Social Virtues and the Creation of Prosperity*, Free Press, New York, 1995.

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

[8] ITU-T, *Specification of Abstract Syntax Notation One (ASN.1)*, Recommendation X.208, Geneva, 1988.

[9] Jøsang A., A Logic for Uncertain Probabilities, Int. J. of Uncertainty, *Fuzziness and Knowledge-Based Systems*, Vol. 9, Issue 3, pp. 279–311, World Scient. Publishing, London, 2001.

[10] Klyne G., Survey of Papers from the iTrust 2003 and 2004 Trust Management Conferences, 2004, http://www.ninebynine.org/iTrust/iTrust-survey.html.

[11] Kovač D. and Trček D., Qualitative trust modeling in SOA, *J. Syst. Archit.*, Vol. 55, No. 4, pp. 255–263, Elsevier, 2009.

[12] Linke A. and Manteau L., Report on the EU Research Project Inspired: The future of Smart Cards, 2005, http://www.inspiredproject.com/documents/20050728-paper-isse2005-final.pdf.

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

[14] Muir B.M., Trust in automatition-I - Theoretical issues in the study of trust and human intervention in automated systems, *Ergonomics*, 37(11), pp. 1905–1922, 1994.

[15] Muir B.M. and Moray N., Trust in automatiotion-II - Experimental studies of trust and human intervention in a process control simulation, *Ergonomics*, Special Issue, Cognitive ergonomics, 39(3), pp. 429–460, 1996.

[16] Nisbett R.E., Krantz D.H., Jepson C., Fong T.G., Improving inductive inference, in Kahneman D., Slovic P., Tversky A. (Eds.), Judgement under uncertainty: Heuristic and Biases, pp. 445–459, Cambridge University Press, Cambridge, 1982.

[17] Osterwalder D., Trust Through Evaluation and Certification?, *Soc. Sci. Comp. Review*, 19(1), pp. 32–46, 2001.

[18] Piaget J., *Judgment and Reasoning in the Child*, Routledge, London, 1999.

[19] Reding V., Safety on the Net. Int. High Level Research Seminar on Trust in the Net, Vienna, 2006, http://ec.europa.eu/comm/commission_barroso/reding/docs/speeches/viennaq_20060209.pdf.

[20] Trček D., A formal apparatus for modeling trust in computing environments, *Math. and Comp. Modelling*, 49(2009), pp. 226–233, Elsevier, 2009.

[21] Trček D., Ergonomic Trust Management in Pervasive Computing Environnets (invited talk), *Proc. of ICPCA ’10*, Maribor, pp. 1–6, 2010.

[22] TRUSTe, Security Guidelines. TRUSTe, San Francisco, 2005, http://www.truste.org/pdf/SecurityGuidelines.pdf.

[23] Wang Y. and Vassileva J., Trust and Reputation Model in P2P Networks, *Proc. of the 3.rd Int. Conf. on Peer-to-Peer Computing*, pp. 150–1554, 2003.