Qualitative Trust Dynamics Algebra for Trust Management in Pervasive Computing Environments

DENIS TRČEK
Laboratory of e-media
Faculty of computer and information science
University of Ljubljana
Tržaška cesta 25, 1000 Ljubljana
SLOVENIA
denis.trcek@fri.uni-lj.si http://www.fri.uni-lj.si/si/katedre_in_laboratoriji/informatika/e-mediji/

Abstract: Trust management is turning out to be essential for further and wider acceptance of contemporary IT solutions. It was first addressed some ten years ago when the suggested approaches at that period were actually tackling security and not trust directly. Later, more advanced methodologies emerged that were based on Bayesian statistics, and these were followed by Dempster-Shafer theory of evidence and its derivative, subjective algebra. In addition, some attempts were made that were based on game theory. However, trust is a manifestation of reasoning and judgment processes. It has to be treated in line with this fact and has to be adequately supported from technological point of view. Therefore, on the basis of experiments, a complementary methodology called qualitative trust dynamics algebra (QTDA) has been developed, which addresses the core of trust phenomenon. It complements existing methodologies and, together with the appropriate conceptual model, enables technological solutions for trust management in pervasive computing environments.

Keywords: web services, pervasive computing, security, trust management, human factor modeling, qualitative trust algebra.

1. Introduction

Trust in information systems is playing an increasingly important role. If users are supposed to use various e-services, especially those sensitive ones, they have to trust these e-services. It might appear at the first glance that this may be a bit artificial or overstated issue, but the reality shows this is not the case. It can be anticipated that this issue will play an increasingly important role, because we are entering the era of pervasive computing, where we will be surrounded by numerous computing devices. Trust in this case will not be just a matter of security and privacy, but increasingly of safety.

Also the EU Commission has recognized that trust in e-services is an important issue that requires attention; recognizing that there is not enough trust in the network [1,2] it has launched research initiative and some recent projects in this area are the following ones:

- ICE-CAR, which was aimed at providing technology for secure use of internet in commercial and administrative domains (in fact, this was one of EU PKI initiatives).
- ECRYPT, which was focused on integration of crypto-primitives, stenography and crypto-protocols.
- INSPIRED, which was focused at enhancing smart-card technology into second generation trusted personal device for security and privacy.
- PRIME, which was aimed at providing solutions for privacy assuring identity management through appropriate interfaces, cryptography and ontologies.
- ITrust, which was a forum for cross-disciplinary investigation of trust; it was based on the fact that trust was a key enabler for meaningful and mutually beneficial interactions.
- TrustCoM, which was a framework for trust, security and contract management in dynamic virtual organizations; the framework focused on an open source reference implementation building on public specifications.

The above list well reflects the situation in the area of trust management, where trust is often used interchangeably for security and privacy. However, trust is a psycho-sociological phenomenon on its own and has to be treated accordingly (which is also the case with some of the above mentioned projects).

This paper focuses on trust as a psycho-sociological phenomenon. It provides relevant definitions and presents a formal model that serves as a basis for computationally supported trust management. This model enables application of various methodologies, where currently in the literature only the quantitative ones prevail. However, our research implies that there is a need for a complementary methodology, which should be qualitative one.

The paper is structured as follows. In the second section an overview of the field is given. The basic definitions follow in the third section. In the fourth section the model for computational support of trust is presented together with qualitative algebra. There is a conclusion in the fifth section, while the paper ends with references and acknowledgements.

2. Overview of the field

Research of trust (and related issues) can be divided into two epochs. The first one took place during the 90s of the former century, while the second one started at the beginning of the current decade. Some most notable representative methodologies intended for supporting trust of the first epoch are the following (it is interesting that these epochs roughly coincide with classical internet services on one side, and advanced solutions like services oriented architectures on the other):

- Platform for Internet Content Selection or PICS – this approach was about access control related to web-sites filtering [3].
- PolicyMaker – trust management was aimed at addressing trust management problems in network services by bounding access rights to the owner of a public key, whose identity was bound to this key through a certificate [4].
- Trust Establishment Module, which was a Java based solution with appropriate language, similar to PolicyMaker, and which enabled trusting relationships between unknown entities by using public key certificates [5].

Many other early approaches are described in detail in a survey by Grandison and Sloman [6], and the reader is referred to it for additional details.

With regard to the most important advancements of the second epoch, the following ones should be mentioned (more detailed discussion can be found in a survey by Josang, Ismail and Boyd [7]):

- Trust management has been extended to a new concept (aggregate), which is reputation management. As opposed to trust systems, which usually take subjective and general measures as input, reputation systems produce a score that reflects entity's public reputation score as seen by the whole community.
- Trust has been seen as a complementary, soft security mechanism to traditional ones. While traditional mechanisms typically protect resources from malicious users, trust systems provide protection against those that offer subverted resources.

With regard to existing methodologies that are used for trust and reputation management, the most simple are those that sum or average ratings of a society (such cases are eBay's and Amazon's rating systems). More sophisticated methodologies are based on Bayesian statistics, where the newly calculated reputation value (a posteriori score) is obtained by combining past values (a priori scores). The reputation score is given by standard beta probability density function (B PDF) with parameters α and β (these parameters represent the amount of positive and negative scores) [8]. Standard B function is defined as follows (p denotes probability, $\alpha, \beta > 0$, while there is a restriction $p \neq 0$ if $\alpha < 1$ and $p \neq 1$ if $\beta < 1$):

$$B_{\alpha,\beta}(p) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha) * \Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1}$$

When a system is initiated and no data exist, the standard B PDF results in a uniform distribution ($\alpha = \beta = 1$). After r positive outcomes and s negative outcomes, the B PDF has parameters $\alpha = r + 1$ and $\beta = s + 1$. On this basis concrete probability expectation value can be obtained:

$$E(p) = \frac{\alpha}{\alpha + \beta}$$

As this expected value is probability itself, this means that the above equation actually expresses uncertain probability of positive outcomes. In case of $E(p) = 0.7$, this value means that the relative frequency of positive outcomes of an entity in question is most likely 0.7.

By extending the Bayesian statistics, Dempster-Shafer theory of evidence has been developed (it is a generalization of the Bayesian theory of subjective probability [9, 10]). This theory defines a set of possible states as a frame of discernment Θ, where exactly one state is assumed to be true at any time. If a frame of discernment is given by atomic states x_1, x_2, x_3, x_4, and a compound state $x_5=\{x_2, x_3\}$, this means that $\Theta = \{x_1, x_2, x_3, x_4, \{x_2, x_3\}\}$. Then the belief mass is assigned to every state. In the case of, e.g. x_5 it is interpreted as the belief that either x_2 or x_3 is true, but the observer cannot determine the exact sub state that is true. Based on belief mass belief function is derived, which is interpreted as a total belief that a particular state is true, be it atomic or compound.

Dempster-Shafer theory has served as a basis for Jøsang's subjective algebra [8]. Jøsang's algebra preserves mathematically sound basis; it contains equivalents to traditional logical operators, but it also introduces new ones like recommendation and consensus. An opinion ω is modeled with a triplet (b, d, u), where b stands for belief, d for disbelief and u for uncertainty. Each of these elements gets its continuous values from [0, 1], such that $b + d + u = 1$. For example, an agent's opinion can be expressed as $\omega = (0.6, 0.3, 0.1)$.

While the Bayesian theory requires exact probabilities for each question of interest, belief functions enable to base degrees of belief for one question on probabilities for a related question. Further, in belief theory the sum of probabilities over all possible outcomes not necessarily adds up to 1 - the remaining probability is interpreted as uncertainty.

In the survey by Jøsang's, Ismail and Boyd, fuzzy and flow methodologies are also described. Fuzzy methodologies deploy principles of multi-valued logic derived from fuzzy set theory introduced by Lotfi Zadeh (one example of fuzzy logic based methodology for trust management was proposed by Manchala [11]). The second kinds of methodologies are flow methodologies and they depend on the assumption of transitivity of trust. In this case a trust value is calculated on the basis of chained trust values of particular entities that constitute such chain (an example is the Appleseed algorithm [12]).

3. The definition of trust

It is quite straightforward that trust is the primary phenomenon, while reputation is its derivative. True, reputation can be taken as a starting point by a certain agent when this agent has no prior experience with another agent, but this does not change the basic principle, which is that reputation is based on trust estimates of the whole community.

It can be seen from the above discussion that it is first necessary to properly define trust:

- Trust is assured reliance on the character, ability, strength, or truth of someone or something (Merriam-Webster dictionary).
- Trust is the subjective probability by which an individual expects that another individual performs a given action on which its welfare depends (reliability trust) [7].
- Trust is the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible (decision trust) [7].

The above definitions well describe the essence of trust, however, for the application in the IT area the definition provided by Dorothy E. Denning at the beginning of nineties seems to be the most appropriate: *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.*

4. Qualitative trust dynamics algebra

Trust is primarily a manifestation of reasoning and judgment, which implies the need to include the relevant research in the field of psychology. Piaget's has done some fundamental work in the area of reasoning and judgment [13]. Therefore his work will be the basis for our conceptual model with the following elements [14]:

- Irrationality. It should not be assumed that each agent is able to rationally assign values to trust.
- Trust differentiation. Trust evolves into various forms. The reasons are bad communication capabilities of an entity, expressing trust, bad perceiving capabilities of a targeting entity, and trust being mediated intentionally modified.
- Action binding. An opinion can serve as a potential (a basis) for agent's deeds.
- Feed-back dependence. Trust is not a product of an independent mind. Being forced to adopt a certain kind of behavior, an agent may change opinion about the very same kind of behavior.
- Temporal dynamics. Agent's relation towards object / subject being trusted is a dynamic relation and it changes with time.
- Context dependence. Agent's trust is a function of a context (environment). The first level of context dependence deals with agent's trust by exclusion of social interactions. The second level of context dependence includes social interactions.

Based on the above basic elements, the conceptual model, intended for computational support of trust, is presented in Fig. 1, where Δ denotes the set of deeds of agents in a society, Ω denotes the set of all trust values in this society, while T denotes time. Thus the context is defined as $\Gamma = \Omega \times \Delta \times T$. Further, the three functions (φ, η, μ) define the two feed-back loops between agent's trust and the context.

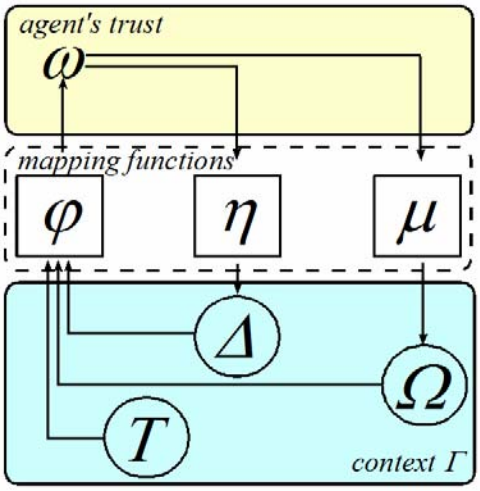

Figure 1: Mathematical model of trust phenomenon

It is time now to introduce qualitative trust dynamics algebra (QTDA) [15]. This algebra currently addresses the context $\Gamma = \Omega$.

According to QTDA, trust is a relationship between agents A and B, which is denoted by $\omega_{A,B}$, which means agent A's attitude towards agent B. Further, by focusing on actual trust within a certain context the following can be observed:

- in general, trust relation is not reflexive;
- in general, trust relation is not symmetric;
- in general, trust relation is non-transitive.

The basic premise of QTDA is that it is hard for an ordinary person to evaluate it in quantitative terms (many people have problems even with such basic concepts as probability [15]). Therefore trust as a relationship is qualitatively "weighted" with qualitative weights being "trusted", "untrusted" or "undecided".

Propagated trust in social interactions is represented with trust matrix M, where elements $\omega_{i,j}$ denote trust relationships of the i-th agent towards the j-th agent, and have values 1, or 0 or -1 to denote trusted, undecided and untrusted relationships. If a relation is not defined, it is denoted by "–," meaning that an agent is either not aware of the existence of another agent, or does not want to disclose its trust.

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

In such matrices, columns represent a trust of a society towards a certain agent; therefore they are referred to as trust vectors. As matrices can be equally represented by graphs, it should be a straightforward task for a reader to derive appropriate trust graph of a certain society on the basis of a given matrix.

The trust dynamics in a given society is dictated by initial trust values of agents, and trust operators that govern their behavior. There are now going on experiments with some new operators within QTDA, but so far the following three have been defined (their appropriateness is based on linguistic grounds – words that describe them are very frequently used in many languages, and consequently various cultures):

- optimistic judgment operator which results in the most positive judgment value in a trust vector, and is denoted by the symbol "↑";
- pessimistic judgment operator which results in the most negative judgment value in a trust vector, and is denoted by the symbol "↓";
- opportunistic (centralistic) judgment operator which results in an "average" value of a trust vector, and is denoted by the symbol "⇌".

$\omega^-_{i,k}$	$\omega^-_{j,k}$	$\omega^+_{i,k}$, $\uparrow_i$	$\omega^+_{i,k}$, $\downarrow_i$	$\omega^+_{i,k}$, $\rightleftharpoons_i$
1	1	1	1	1
1	0	1	0	0
1	-1	1	-1	0
1	-	1	1	1
0	1	1	0	0
0	0	0	0	0
0	-1	0	-1	0
0	-	0	0	0
-1	1	1	-1	0
-1	0	0	-1	0
-1	-1	-1	-1	-1
-1	-	-1	-1	-1
-	1	-	-	-
-	0	-	-	-
-	-1	-	-	-
-	-	-	-	-

ISSN: 1790-5109

ISBN: 978-960-474-107-6

In the above table, which defines precisely the trust operators, the trust operation is denoted by $\omega^{+}_{i,k} = op_i$ $(\omega^{-}_{i,k}, \omega^{-}_{j,k})$, where $op_i = \{\uparrow, \downarrow, \rightleftharpoons\}$ and "-" denotes pre-operation value, while "+" denotes the resulting value of an operation.

Now let us assume a society with four agents, where the first agent is a dumb agent, while agent 2 is ruled by optimistic operator, and agents 3 and 4 are behaving according to pessimistic operator. If the initial distribution is as given in the left matrix below, then in the next step the resulting trust values are given in the right matrix:

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

The above example is a very basic one and it only serves as a starting point. Despite the fact that currently our model excludes η and the domain of deeds Δ, the situation is already becoming very complex because of the following reasons:

- The above deterministic operators are not a permanent characteristic of an agent even in the same context, so an agent can change from e.g. optimistic to opportunistic.
- New operators are now being investigated and are already being added to QTDA; current research shows that some of the new operators will have to be non-deterministic.
- Currently, it is assumed that the effect of other opinions is instantaneous. However, we are introducing and modeling the so called *convincing threshold function* to take this into account (this function models required influence time for an agent change its mind).
- It is currently assumed that there is no mental anchoring, i.e. that values from the past do not influence agent's current opinion. But a more realistic assumption (also supported by research done by e.g. Makridakis [16]) is to use exponential weighting.

Now even with simplifications stated above, some interesting results can be found [17]. Suppose our community consists of 100 agents, where the initial percentage of agents using optimistic operator varies from 10% to 90% (we change percentages of pessimists and centralists, starting with 10% optimists, 10% pessimists and 80% centralists initially, and ending with 90% optimists, 10% pessimists and 0% centralists). Further, we allow that every few steps (say every 10 steps) a certain percentage of agents (in our case 10%) may change their trust value or their operator. The whole simulation lasts 500 time increments.

Using such conditions, it is interesting to see that the number of optimists converges to 1/3 of the whole population, while smoothed curves seem to be described (governed) by exponential functions (see Fig. 2 [17]).

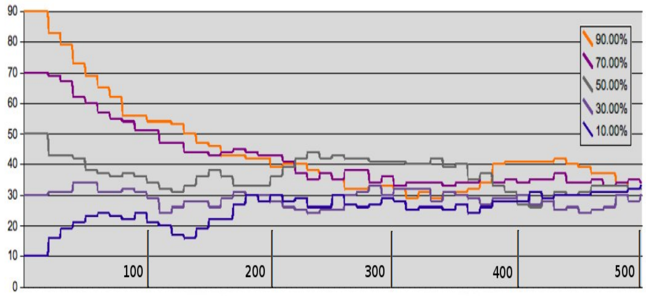

Figure 2: A case of trust dynamics using QTDA (the horizontal axis denotes the simulation steps, the vertical axis the percentage of optimists in a society)

It can also be seen from the above figure that using only these three basic operators the society converges quickly after a change is applied, however relatively small perturbations (10% changes of operators or trust values) have significant impact on the whole community.

5. Conclusions

Trust issues came to the forefront not only in the internet to promote and support e-activities, but also in a wider society. This paper presents a methodology called qualitative trust dynamics algebra (QTDA) that is based on research that indicates that people prefer qualitative metric when it comes to trust. Therefore QTDA complements other methodologies that are based mostly on the assumption of rational behavior of agents. It has been demonstrated in this paper how QTDA can be used to analyze and support trust in virtual (and also simple real) settings.

Future work will be focused on adding more sophistication to the QTDA by extending the experiments that have already been performed so far. As mentioned, QTDA will not be usable only to support trust management in computerized environments (our current application of QTDA is called trustGuard and its details can be found in [18]),

ISSN: 1790-5109

ISBN: 978-960-474-107-6

but hopefully also to manage agents in a way that would result in more trustworthy societies.

References:

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

[2] Reding V., *The need for a new impetus to the European ICT research and innovation agenda*, Int. High Level Research Seminar on "Trust in the Net", Vienna, 9th February, 2006.

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

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

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

[6] Grandison, T., Sloman, M., A Survey of Trust in Internet Applications, *IEEE Communications Surveys*, Vol. 3, No. 4, pp. 2-13, 2000.

[7] Josang A., Ismail R., Boyd C., A survey of trust and reputation systems for online service provision, *Decision Support System*, Vol. 2007, No. 43, pp. 618-644, Elsevier, 2007.

[8] Jøsang, A., A Logic for Uncertain Probabilities, *Int. Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 9(3), 279-311, 2001.

[9] Dempster, A.P., A generalization of Bayesian inference, *Journal of the Royal Statistical Society*, Series B, Vol. 30, No. ?, 205-247, 1968.

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

[11] D.W. Manchala, Trust metrics, models and protocols for electronic commerce transactions, *Proceedings of the 18th Int. Conference on Distributed Computing Systems*, pp. ?, 1998.

[12] Ziegler C.N., Lausen G., Spreading activation models for trust propagation, *Proc. of the IEEE International Conference on e-Technology, e-Commerce, and e-Service (IEEE '04),* Taipei, 2004.

[13] Piaget J., *Judgment and reasoning in the child*, Littlefield Adams, Totowa 1969.

[14] Trček D., Managing trust in services oriented architectures, *Proceedings of the 8th WSEAS International Conference on Applied Informatics and Communications (AIC'08)*, pp. 23-28, Rhodes, 2008.

[15] Trček D., A formal apparatus for modeling trust in computing environments, *Mathematical and Computer Modeling*, Volume 49, Issues 1-2, pp. 226-233, Elsevier, 2009.

[16] Makridakis, S. et al, *The Forecasting Accuracy of Major Time Series Methods*, John Wiley & Sons, Chichester, 1986.

[17] Zupančič E., *Managing Trust in IS by Using computer Simulations*, FRI UL, Ljubljana, 2009.

[18**]** Kovač D., Trček D., Qualitative trust modeling in SOA, *Journal of systems architecture,* Volume 55, Issue 4, pp. 255-263, Elsevier, 2009.

Acknowledgements

The author would like to thank ARRS (the Slovene Research Agency) for financially supporting the research presented in this paper through research program P2-0359 and project J2-9649.