Considerations about Modelling Trust

Dr. Ioan Despi, Lecturer
University of New England, Armidale, Australia
Dr. Lucian Luca, Associate Professor
"Tibiscus" University, Timisoara, Romania

REZUMAT. Un concept important în software şi în reţele de orice fel este încrederea, interpretată ca o relaţie între agenţii participanţi. Combinată cu neîncredere şi nesiguranţă, atunci când se modelează reţele hibride cu agenţi umani şi software, ea oferă un cadru atractiv pentru diferite modelări matematice. În special, proprietăţile de tranzitivitate joacă un rol central în cercetarea noastră, aceasta putând fi modelată cu algoritmi pentru a calcula propagarea încrederii şi neîncrederii în reţele.

1 Introduction

"*The web is more a social creation than a technical one. I designed it for a social effect — to help people work together — and not as a technical toy. The ultimate goal of the Web is to support and improve our weblike existence in the world. We clump into families, associations, and companies. We develop trust across the miles and distrust around the corner.*" (Tim Berners-Lee, Weaving The Web)

Trust is the essential component of interactions in everyday life, in businesses and, more recently, in *online* life provided by computers. Often understood in a vague and unsystematic way, trust is present in all aspects of human and computer life. The humans strive to put it to the tools they create. The concept of trust shaped all aspects of human life from the early beginning but many of the well-established strategies for asserting and representing trustworthiness can no longer be used in the computerised world we live now. New ways are opened by the emerging technologies,

and new challenges face the scientists. The World Wide Web "will soon reflect the full complexity of trust relationships among people, computers, and organisations" [KR97]. Computers networks and Internet (with all its ingredients) are increasingly shifting us from the old, familiar and direct style of interacting. According to The paradigm of the last decade is collaboration. Nowadays we may collaborate online with people or organisations we have never met and/or heard of before. After finishing our projects, probably we'll never meet them again. Collaboration means trust, and because we deal with persons and machines we never met before, we have to compute it by using algorithms. Our problem is to determine how much one person or machine – say *agent* – in a network should trust another person or machine, on the same network or from elsewhere on the Internet.

We start by presenting the nature of social and machine belief, trust and reputation (Section 2), then we continue with the new main places where trust is required (Section 3), then in Section 4 we outline our model, and we conclude in Section 5.

2 Belief, Trust, and Reputation

Computers and Internet imply a lot of interactions between humans, machines and programs (in a word: *agents,* and the system is called *MAS* – Multi-Agent System) for needed resources (information, services, or tangible goods). These interactions are risky, as agents make agreements, which may or may not be fulfilled, so agents must predict outcome of interactions and must predict and avoid unreliable agents. Belief, trust and reputation model these predictions.

A *belief* is an assumed truth. It means it can be challenged, reformed and changed. The relations must be based on *trust*: agents must be confident that other agents will do what they have been asked and only what they have been asked. A *reputation* is "an expectation about an agent's behaviour based on information about or observations of its past behaviour. " [AH00]

Agents create *beliefs* to anchor their understanding of the world around them. Once they have formed a belief, they will tend to persevere with that belief. There are many types of belief. One of the simplest beliefs is that something (e.g., F) exists (*existence*). If an agent is such that what it perceives is an internal inference of what happens in the outer world, the first belief in its knowledge base Δ is that what it perceives truly exists. The existence can have temporal and morphological aspects: F can come into existence at a point in time, it can change into something else (F becomes

G), or it can even disappear. *Association* (F : G) means that agents understand things in term of other things, and the knowledge base should include a map of similar things (F is *like* G). Equivalence (F= G) is when agents assume things are more or less the same, *causation* (F → G) is the logical implication, and *enaction* (F happens) occurs when agents should accept an imperfect world and believe in the flow of time and the change of the world around them. Based on their attitude to the world and on other agents around them, agents can use two different methods to build beliefs.

1. *Self-generated beliefs*. They are those beliefs agents create themselves, by experience and/or reflection and by distrusting experts or other authorities.
    a. *Experience* is the ultimate method an agent has to finding the truth. Experience means observing and trying things out in practice and getting a lot broader range of evidence before committing to a belief.
    b. *Reflection.* This is the opposite to experience in that it is internal rather than external, and it can also be complimentary, as an agent either reflects after an experience or it seeks experiences after internal reflection. Reflection includes general musing about things and building internal models which help to explain the world around.
2. *Externally-generated beliefs*. The alternative to finding things out is to take on board things the other agents have found out. Agents who generally prefer to accept beliefs from other agents have a greater need for a sense of control.
    a. *Experts* are agents who have proven themselves to have knowledge in particular areas, by means of special qualifications and skills. Agents who seek experts are relatively pragmatic: they trust but not blindly; they a re looking for someone to help in a specific area.
    b. *Authority* differs from an expert because of their position and not because any other reasonable proof that they know well what they are talking about. Agents who believe (only) authorities are followers and a gullible and easy to persuade by hackers or malicious programs.

A good agent is a combination of all of these. When a hacker or an intruder is seeking to change beliefs, it will try to find out where the agents get their beliefs from. If they come from self-generated beliefs, then hacker gives to them experiences or rational arguments; if they are more external,

then pose as an expert or authority, or bring in someone who can fulfil the appropriate role.

The problem of belief change appears whenever an agent's model of the world needs to be modified by the addition of new information describing changes in the world or by showing that the initial set of beliefs was incorrect. Formally, given an initial knowledge base Δ and a new piece of information δ to be incorporated into it, what should the new database be? If δ is consistent with Δ, then the new database is simply the addition of δ to Δ. The operation of incorporating a new piece of information into an existing database can be differentiate in belief revision and belief update. *Belief revision* means that beliefs may have been wrong and in need of revision, whereas *belief update* says that the beliefs were correct, but the world has in the meantime evolved and the beliefs have to be updated [KM91].

Based on the role assigned in the revision process to the agent's reasons for holding its beliefs, there are two main approaches to believe revision, foundation and coherence. In the *foundation theory of belief revision*, the agent's beliefs are seen as a structure transcending the purely logical relations between them: starting with a set of basic or self-justified beliefs, other beliefs are seen as justified by some other beliefs, and so on. In the revision process some basic beliefs can be eliminated, and so the revision will propagate in the entire hierarchy of beliefs. In the *coherence theory of belief revision,* the main goal of the agent is to maintain the overall coherence of its beliefs when new information arrives [Gar90].

The dictionary defines *trust* as "the trait of trusting; of believing in the honesty and reliability of others" (http://www.wordreference.com). As synonyms for trust, we get confidence, dependence, faith, hope, reliance, and stock; as related words, we get assurance, certainty, certitude, belief, credit, sureness, entrustment, positiveness, credence. The complex subject of trust has been explored for a long time and by a large palette of disciplines, from economics, psychology, sociology, history, philosophy to computer science. Each discipline approached the subject from a personal point of view and tried to produce definitions and delimitations. Moreover, the concept of trust is unclear in philosophical, sociological or technical sense also [Sel97]. For instance, "trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another" [RSBC98], or "an individual's belief in, and willingness to act on the basis of, the words, actions, and decisions of another" [LMB98], or [trust] "…begins where predictions end" [LW85], etc.

In psychology, trust is often considered to be little more than an individual psychological state that has more to do with a specific individual and his psychological and sociological make-up than with some real-life state of affairs [LW85]. The sociological studies on trust make distinction between trust in people and trust in abstract systems. Interpersonal trust is based on mutual involvement and in the faith in the integrity of the other person. The abstract system is, for instance, the user interface through which the user accesses the web and trust in the abstract systems is a personal and subjective feeling of day-to-day security, which in turn forms the basis for social life [Gid89]. Philosophically, trust is to be separated from confidence and faith, even if one can find a partially overlapping.

Trust is connected with *vulnerability*, it is "the condition in which one exhibits behaviour that makes one vulnerable to someone else, not under one's control" [Zan72]. Without vulnerability, there is no need for trust. An agent is making himself vulnerable in order to accomplish a goal. Trust (cooperative) is also connected with *distrust* (competitive), defined as "the confident expectation that another individual's motives, intentions, and behaviours are sinister and harmful to one's own interest" (http://www.beyondintractability.org/m/distrust.jsp). The relationship between trust and distrust is not a simple one. One approach started with a full-trust relation and considered distrust as a negative trust, but this raised a lot of problems, both philosophical and algorithmic (they got negative probabilities, for instance). We'll come with a different solution, combining trust, distrust and uncertainty.

The primary property of trust is *transitivity*: if agent X trusts agent Y and agent Y trusts agent Z, then agent X trusts agent Z, but we do not believe distrust is strictly transitive. The second property of trust is *composability*, if agent X gets many recommendations about how much to trust agent Y, X has to compute (to compose) the information to decide whether or not to trust Y (or to decide the degree of trust for Y). Other properties for trust are *personalisation,* that is two agents X and Y can have different degrees of trust regarding another agent Z, and *asymmetry*, the degree X trusts Y is not the same as the degree Y trusts X..

T^3 group led by Rino Falcone (http://www.istc.cnr.it/T3/) study the trust concept from many different points of view. In their socio-cognitive model, trust is firstly a mental attitude. Only a cognitive agent can trust another agent and one trust another only relatively to a goal, i.e. for something it wants to achieve, because trust is the mental counter-part of delegation. If X is the relying agent, who feels trust, and Y is the agent which is trusted, then *X has a goal G and tries to achieve it by using Y.*

Secondly, then X has some specific beliefs, such as *competence* belief and *disposition* belief (prototypical components of trust as an attitude towards Y), *dependence* belief, and *fulfilment* belief. The beliefs and the goal G define *X's trust in Y* in delegation.

The net result of this increased mixture of perspectives is the fact that there are many different types of trust and it means something different in each discipline or context. The cumbersome point at which theories start to diverge from one other is the identification of the grounds on which acts of trust may be based on. For instance, a group of economists or computer scientists will see trust as based on calculations, in contrast to a group of sociologists who will base trust on common values and moral orientation [Dal05].

Reputation is closely related to trust. It has a global feature, as opposed to trust which is viewed from a local and subjective perspective, and a subjective feature, that is reputation is an opinion. A reputation can be defined as "an import of the past behaviour of an entity" [DeDa03]. Reputation typology comprises context, personalisation, individual or group, direct or indirect (prior-derived, group-derived and propagated) [Mui02]. Reputation of X can be computed as the average trust of all other entities towards X. An agent X can evaluate the reputation of another agent Y, either based on its own experiences (with Y) or based on the evaluation (of Y) by others. In the former, if agent Y is cheating, the agent X can be cheated a large number of times before it is able to discover it. In the latter, X has to verify the information it receives from peers about Y. Sometimes reputation is based on *recommendations*, "an expressed opinion of an entity that some another entity is reputable which opinion the recommender is responsible for" [Gri04] and reputation is the mean of the recommendations received by an agent [DeDa03]. Recommendations are contextual, for instance an agent can get different recommendations for its different attributes. A good example of system based on reputation is eBay (www.ebay.com).

From our point of view, trust is built from beliefs and reputation, "…trust is a bet about the future contingent actions of others" [Szt99]. One can notice that there are two bricks in this definition, belief and commitment: a person believes that the trusted person will act in a certain way; trust occurs when that belief is used as the foundation for making a commitment to a particular action. Trust management is an important topic (and a young field), as indicated by the substantial number of research projects that have been initiated in the last decade, many trust-modelling technologies, many metrics for empirical validation, and the lack of unified

research direction. It is "the activity of collecting, codifying, analysing and presenting evidence relating to competence, honesty, security or dependability with the purpose of making assessments and decisions regarding trust relationships for Internet applications" [Gra01]. An agent must build trust models that are reliable, generic, efficient, adaptable, scalable, and flexible.

3 Contexts

The main place where trust is required in this changing world is electronic commerce. By its nature, e-commerce uses and has to build trust between partners that have never traded with each other before. One approach in the literature is to consider trust in relation with the history of exchanges between agents, as in [KBCS00], but a main feature of e-commerce is globalisation and first trade situations, so trust can be build through electronic trade-procedure, as presented in [BLW99]. Another approach consists of interpreting trust-building services as a generalisation of the services of a trusted third party (TTP) in public key infrastructure (PKI), which is using digital certificates [TT00, TT02, Tan03]. The key point of the model is that an agent only engages in a transaction if its level o f trust exceeds his personal threshold.

One of the new trends of the web is the proliferation of a number of web-based services that try to help *netizens* develop networks of friends, friends of friends, to establish new personal contacts or even better business contacts. The given name for these services is *social-networking sites* and their goal is to help netizens build new friendships by connecting people to new people with similar interests or requirements through the web. Generally, to use these services, which are mostly free, one just has to feed in her personal/professional details and register with them. Once registered with a service, she can start building the network by inviting other members to join the service.

Web-based social networks (WBSN) have disseminated rapidly since their inception in the mid-90s and they represent a challenge to traditional ways of thinking
about social networks. For the first time, the scientists have the opportunity to research in vivo huge amounts of individuals connected in a network without using simulation but mathematical and structural types of analysis. Examples of such popular networking sites are *Orkut* (http://www.orkut.com/index.html), a service being projected as the one

affiliated to Google, *LinkedIn* (https://www.linkedin.com/), a service that targets professionals/business people, *Tickle* (http://tickle.com), *CouchSurfing* (http://www.couchsurfing.com/), *Hi5* (http://hi5.com), *Friendster* (http://www.friendster.com/index.jsp), etc.

Another trend is an emerging technology that allows web authors define their relationships to the authors of other sites. "A *blog* (weB LOG) is basically a journal that is available on the web. The activity of updating a blog is called *blogging* and someone who keeps a blog is called a *blogger*. Blogs are typically updated daily using software that allows people with little or no technical background to update and maintain the blog" (Matisse Enzer, http://www.matisse.net/files/glossary.html). Postings on a blog are almost always arranged in chronological order with the most recent additions at the beginning. Usually, a blog has a component called *blogroll*, where the blogger inserts links to other blogs that he regularly reads. In recent years, *blogs* and *blogrolls* have become the fastest growing area of the Web.

By just providing a link to another blog, a reader will not get any idea about the relationship the blogger has with the target blog's author. The technology XFN (XHTML Friends Network) addresses this issue by providing a simple way to represent human relationships (friendship, professional, geographical, family, romantic, etc.) using hyperlinks. XFN enables web authors to indicate their relationship(s) to the people in their blogrolls simply by adding a ***rel*** attribute with a space-separated list of relationships to their `<a href>` tags. The possible values of relationship are pre-defined and in most cases are deliberately open to interpretation: *aquaintance, friend, met, co-worker, collegue, co-resident, neighbor, child, parent, sibling, spouse, muse, crush, date*, *kin, contact, me*, and s*weetheart*. For instance, suppose John is a friend of yours whom you have met in real life and he owns the site http://www.goodnews.com. When you add that site to your list of links, you can specify that its owner is a friend that you have met in real life. The link that is created will be of the form: John

XFN Graph (http://xfngraph.sourceforge.net/) is an open-source project to build a tool for visualising the relationships between bloggers who mark up their blogrolls with XFN. XFN Graph uses this information to draw spider diagrams showing how sites link to one another.

The *Friend Of A Friend* (FOAF) project is about creating a Web of machine-readable homepages describing people, the links between them and the things they create and do (http://foaf-project.org/). If one publishes documents in the FOAF format, then the machines will be able to use them;

for instance, the machines will follow *see also* links from one document to another.

The framework is based on a set of definitions designed to describe people, membership in groups, and social connections, and used to build the dictionary of terms able to express queries about the world. The documents are produced using the XML syntax, enhanced with the conventions of RDF (Resource Description Framework). Some examples of constructions are: `foaf:Person`, `foaf:Document`, `foaf:Image`, alongside with some properties of those things, such as `foaf:name`, `foaf:mbox`, `foaf:homepage` etc., as well as some kinds of relationship that hold between members of these categories, such as `foaf:depiction (it r`elates something (e.g., a `foaf:Person`) o a `foaf:Image)`. More details about each term and its use can be found at http://xmlns.com/foaf/0.1

The *trust ontology* (http://trust.mindswap.org/ont/trust.owl) is software written in OWL/RDF that allow people to rate (on a scale from 1 to 10) how much they trust other people, namely 1 means no trust and 10 means total trust. There is no notion of explicit distrust in this ontology.

Another problem is how to provide secure, continuous and efficient connectivity for a mobile unit in an ad-hoc network or even in a structured one (point-of-access based). *Ad-hoc networking* allows enterprises to create spontaneous networks that are coordinated *on-the-fly* using point-to-point technology. Usually, it means a collection of wireless mobile hosts forming a temporary network, without the aid of any centralised infrastructure or administration. Their main areas of application are military domain (mesh-cube), conferences, meetings, lectures, attachments to WLAN, UMTS, networks for cabdrivers and police, and catastrophes.

These networks are based on a fundamental assumption that the nodes will cooperate and not cheat. In a mobile ad-hoc network (MANET), the participants are used to route communication traffic from senders to receivers, every participating node executing a routing algorithm that allows messages to be directed towards the next node along a route to the receiver. The protocols have to take into account the mobility of the participants and the variation in the connectivity between associated parties. The main challenges are the dynamic topology (movement, node failure, energy), heterogeneous and decentralised control, limited resources (bandwidth, energy, processing ability), and unfriendly environment (selfish nodes, malicious attackers). To secure ad-hoc networks means to establish trust relationships in open environments, using an algorithm that evaluates trust among hosts (a host's trustworthiness affects the trust toward the hosts on the route). A related issue is intruder detection and removing, which,

again, will use trust information (the trust opinion of A towards an entity B in a certain context C).

4 The model

Trust evidence is seldom complete and certain so there is a need to compute it between any two participating agents. In our approach, we use a weighted directed graph G(V,E), where vertices are the agents and a single trust relationship can be expressed as an edge $A \xrightarrow{w} B$, where A is the issuer (the trust originator) and B is the trust target. The weight function is

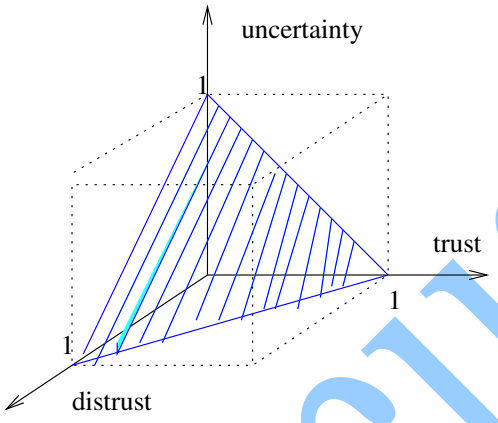
$$w(A,B): V \times V \to S$$

where V is the vertex space (agents) and S is the opinion space. Each opinion in S consists of a *trust* value, a *distrust* value, an *uncertainty* value, and a *confidence* value. The first three values correspond to the issuer's estimate of the target's trustworthiness and the last value corresponds to the accuracy of this estimation. All values are fuzzy values, that is $S = [0,1]^4$ and $\forall s \in S, s = s_B^A = \left(t_B^A, d_B^A, u_B^A, c_B^A\right)$, with

$$t_B^A + d_B^A + u_B^A = 1 \qquad (1)$$

The interpretation is obvious, for instance a high trust value may mean that the target is a trusted agent (a value of 1 means it is for sure). A value of 0 indicates either no previous experiences or just only bad experiences between the two actors. Notice the presence of the uncertainty function, such that trust and distrust for a given opinion do not sum to 1, still there is room for doubt. The above relation also allows us to consider S as $S = [0,1]^3$, getting rid of one of the values *d, t*, or *u,* by computing it as the difference between 1 and the sum of the other two (for instance, d = 1 – t – u). Taking into account the relation (1), the hypercube of all possible values can be reduced to a plane; these three values can be mapped into the interior of an equal-side triangle, a plane passing through points (1, 0, 0), (0, 1, 0), (0, 0, 1). The parameters are not independent, for instance parameter t_B^A is the value of a linear function on the triangle which takes the value 0 on the edge

which joints the uncertainty and distrust vertices and takes value 1 at the trust vertex (sic!).



The confidence value c_B^A is function of the number of direct and indirect experiences between agents A and B and the black list flag. The black list flag is set by the agent to prevent recommendations from the selected set. A high confidence value means that the target agent B has passed a large number of tests that the issuer agent A has set or the two have interacted for a long time and B is not on the black list. At the first contact between the two agents, the confidence is zero. More, it is a time function, so if two agents do not interact for a long period, the confidence will diminish. All four values are set by the issuer agent based on local observations (e.g. monitoring neighbours for evidence of malicious behaviour).

There are two kinds of problems that can be solved with this approach and both use paths in the graph G. If agents A and B are not neighbours in the graph (there is no edge between them), then *w(A, B)* can be computed as a function of the weights of the intermediate nodes (if the path exists) and the most trusted path between agents A and B can be computed as being the one with highest trust values and lowest distrust values of the intermediate nodes. The solution in the literature [JoPo05, TB04] is to use semiring operators to combine the fuzzy values, namely to use $\otimes$ operator to combine opinions along a path, and $\oplus$ operator to combine opinions across paths; in other words, given a path $p = (v_0, v_1, ..., v_n)$ and weights of the path's edges, $\otimes$ is the operator used to

calculate the weight of the path, and $\oplus$ is the operator used to compute the shortest path weight

$$w(p) = w(v_0, v_1) \otimes w(v_1, v_2) \otimes ... \otimes w(v_{n-1}, v_n) \qquad (2)$$

$$d_{ij} = \oplus w(p), \text{ for all paths from i to j}$$

Actually, this is nothing more then an example of using Floyd-Warshall-Kleene algorithm if the model graph G (V, E) has an edge labelling function with values in some star semiring S and we assume w (A, B) =0 for all non-edges (A, B). Recall that in a star semiring $x^* = \sum_{i \geq 0} x^i$,

$(x + y)^* = (x^* y)^* x^*$, and

$(xy)^* = 1 + x(yx)^* y$

5 Conclusions

We introduced the vast problem of trust between agents from different perspectives and sketched a method for computing trust propagation in a formal way. In future work we plan to refine the model and to provide more computational tools, together with practical applications.

References

[AH00] A. Abdul-Rahman, S. Hailes – *Supporting Trust in Virtual Communities*. Proceedings of the 3rd Ann. Hawaii Int'l Conf. System Sciences, vol. 6, 2000

[BLW99] **R.W.H. Bons, R.M. Lee and R.W. Wagenaar** – *Computer-aided Auditing of Interorganisational Trade Procedures.* International Journal of Intelligent Systems in Accounting, Finance and Management, vol. 8 (1999), 25-44

[Dal05] **K. Dalen** - *Trust and Distrust.* Ph.D. Thesis, Department of Comparative Politics, University of Bergen, 2005

[DeDa03] **P. Dewan and P. Dasgupta** – *Trusting Routers and relays in Ad hoc Networks.* Proceeding of the 2003 Int'l Conference on Parallel processing Workshops (ICPPW'03)

[Gar90] **P. Gardenfors** - *The dynamics of belief systems: Foundations vs. coherence theories*. Revue Internationale de Philosophie (172), 24-46, 1990

[Gid89] **A. Giddens** – *Consequences of Modernity*. Stanford University Press, 1989

[Gra01] **T. Grandison** – *Trust Specification and Analysis for Internet Applications*. Imperial College of Science, Technology and Medicine. London, MPhil/PhD Report, 2001, http://www.doc.ic.ac.uk/~tgrand

[JoPo05] **A. Josang and S. Pope** – *Semantic Constraints for Trust Transitivity*. Second Asia-Pacific Conference on Conceptual Modelling (APCCM2005)

[Gri04] **V.S. Grishchenko** – *A fuzzy Model for Context-Dependent Reputation.* Trust, Security and Reputation Workshop at ISWC 2004, Hiroshima

[KBCS00] **P. Keen, C. Balance, S. Chan and S. Schrump** – *Electronic Commerce Relationships: Trust by Design*, Prentice Hall, NJ

[KR97] **R. Khare and A. Rifkin** – *Weaving a Web of Trust*. World Wide Web Journal 2 (1997), 77-112

[KM91] **H. Katsuno and A. O. Mendelzon** – *On the difference between updating a knowledge database and revising it*. Proceeding of the 2nd International Conference on Principles of Knowledge representation and Reasoning (KR91), 1991

[LMB98] **R.J. Lewicki, D.J. McAllister, and R.J. Bies** – *Trust and Distrust: New Relationships and Realities*. Academy Of Management Review, 23, 438-458, 1998

[LW85] **D. Lewis and A.J. Weigert** – *Social Atomism, Holism, and Trust*. The Sociological Quarterly 26, no. 4, 455-471, 1985

[MC96] **D.H. McKnight and N.L. Chervany** – *The Meanings of Trust*. Technical Report MISRC working Paper Series 96-04, 1996

[Mui02] **L. Mui** – *Computational Models of Trust and Reputation: Agents, Evolutionary Games and Social Networks*. PhD Thesis, MIT, 2002

[RSBC98] **D.M. Rousseau, S.B. Sitkin, R.S. Burt, and C. Camerer** – *Not so Different After All: A Cross-Discipline View of Trust*, Academy of Management Review, 23, 393-4004, 1998

[Sel97] **A.B. Seligman** - *The Problem of Trust*. Princeton University Press, New Jersey, 1997

[Szt99] **P. Sztompka** – *Trust: A Sociological Theory*, Cambridge University Press, 1999

[Tan03] **Y. H. Tan** – *A trust Matrix Model for Electronic Commerce*. In P.Nixon and S. Terzis (eds.): Trust Management 2003, LNCS 2692, 33-45, Springer-Verlag (2003)

[TB04] **G. Theodorakopoulos and J.S. Baras** – *Trust Evaluation in Ad-Hoc Networks*. WiSE'04, Philadelphia, 2004

[TT00] **Y. H. Tan and W. Thoen** - *A Generic Model of Trust in Electronic Commerce*, International Journal of Electronic Commerce, vol. 5(2), 61-74, 2000

[TT02] **Y. H. Tan and W. Thoen** - *A Formal Analysis of a generic Model of Trust for Electronic Commerce*, Journal of Decision Support Systems, vol. 33, 233-246, 2002

[Zan72] **D.E.Zand** – *Trust and managerial problem solving*. Administrative Science Quarterly, 17 (2), 1972