TRUST MODEL EVALUATION CRITERIA: A DETAILED ANALYSIS OF TRUST EVALUATION

Author and co-authors

M. Wojcik[1], H.S. Venter[2], J.H.P. Eloff[3]

Author's affiliation

Information and Computer Security Architectures (ICSA) Research Group

Author's contact details

Department of Computer Science, University of Pretoria, Pretoria, South Africa.

hibiki[1]@tuks.co.za

{hventer[2],eloff[3]}@cs.up.ac.za

ABSTRACT

The advent of the internet has resulted in the exponential growth in availability of information as well as the sources from which this information can be gathered. Information has become an asset as well as a vital tool for decision making processes. In order to gain new information, a business is often required to give some information, it is already in possession of, up. This information could be of a sensitive nature and a business needs to know if the source it is exchanging information with can be trusted. Trust models have been proposed to solve this dilemma.

Trust models use logical rules to analyze the nature of interactions. An agent, which is a computer running a trust model, analyzes other agents it comes into contact with and determines a trust level. The trust level is a single value that controls all interactions occurring between participating agents. Values above a certain threshold are seen as trusted and values below are seen as distrusted.

The problem is that these trust models were found to be wide and varied, with no common set of features between them, making it difficult to determine which models address which particular issues of the concept of trust. This paper proposes a set of criteria that is to be used to evaluate various trust models in order to identify the issues addressed by specific models. Four main categories into which these criteria fall have been identified. Due to space constraints one of these is discussed in detail followed by an example analysis of a trust model in order to illustrate how these criteria are used during trust model evaluation.

KEY WORDS

Trust, criteria, trust model, trust evaluation

TRUST MODEL EVALUATION CRITERIA: A DETAILED ANALYSIS OF TRUST EVALUATION

1 INTRODUCTION

Trust and the intricacies thereof has been a topic of interest in disciplines such as sociology, psychology, economics, philosophy and even history [1]. The advent of the Internet and e-commerce has triggered a similar interest in the concept of trust within the discipline of Computer Science. The Internet and emerging technologies has caused a shift in the way business is conducted. Businesses strive to create a virtual presence in order to attempt to take advantage of the inter-networked, world-wide scope the Internet provides. This new environment provides a wealth of new opportunities for gathering information, providing new services and participating in business interactions. However, in the same way that this environment provides new opportunities, it also exposes the participants to new levels of risk. With the existence of risk comes the need for trust.

Several experts in the field have defined trust models in order to allow agents within a computerized environment to establish trust [2], [3], [4], [5]. [6]. An agent in this context refers to a computerized agent that has some form of trust mechanism in place. However, the models that have been proposed are wide and varied, each focusing on different aspects of the trust building process.

The problem with all these wide and varied models is that there is no consistent set of criteria that is upheld throughout making it difficult for an interested party to decide upon a particular trust model to implement. This paper attempts to solve this problem by introducing a set of criteria that can be used to analyse a given trust model. The defined criteria are driven at assisting analysis of current trust models. The criteria, as defined by the author, consist of four main categories which contain various influencing factors within. These four categories are trust establishment, initial trust, updating trust and trust evaluation. Due to space constrains, only trust evaluation is discussed in detail.

The remainder of this paper is structured as follows. The background, section 2, explores the concept of trust and how it is currently formalized by experts in the research field of trust models. Section 3 defines the set of criteria that is to be used to analyse a given trust model. A basic analysis is given in section 4 to illustrate the means in which this criteria is used. Finally, the discussion and conclusion of this paper occurs in sections 5 and 6 respectively.

2 BACKGROUND

Trust models rely heavily on the concept of trust, often modelling human psychological ways of forming, establishing and maintaining the concept. In order to fully understand trust model architecture it is important to first explore and define the concept of trust. This section explores the concept of trust and introduces some work already done in the research field of trust models.

2.1 Trust

Trust is such an intricate part of our daily lives that we use it constantly without even thinking about it. It is because it is such an intricate part of our daily activities that it has stoked such interest. However, a clear definition has been hard to come by mainly because trust is a unique concept to each individual influenced by one’s own beliefs, morals and experiences. It is thus accepted that trust is subjective.

Nooteboom [7] defines trust as a four-place predicate stating that: "Someone has trust in something, in some respect and under some conditions." These predicates refer to: the agent trusting

(someone), the agent being trusted (something), the reason and goals that define the need for trust (respect) and the conditions under which the trust is given (conditions).

This definition can be further expanded by including Golembiewski and McConkie's [8] views on uncertainty and hopefulness. With uncertainty comes risk. Without the existence of uncertainty, there would be no need for the concept of trust, as the outcome will be pre-determined. Trust does neither guarantee success nor does it give a failsafe method of analyzing interactions. Without risk, trust does not exist [7]. Trust models rely on these cognitive definitions of trust in order to implement the concept.

2.2 Trust models

Various concepts of human trust have been quantified in order to formulate system trust. These concepts include those of how humans establish trust and use trust in order to formulate templates of expected behaviour and outcome. Several trust models, focusing on various aspects of human trust have been proposed by various experts in the field [2, 3, 4, 9, 10]. Concepts of human trust that experts in the field of Computer Science have chosen to use, include the means in which human trust is established, the various forms of trust as well as the concept of making assumptions based on specific trust templates. However, system trust is allowed to be more dynamic in nature than that of human trust due to the nature of the environment: that the need for system trust exists.

Mui, Mohtashemi and Halberstadt [9] focus on building trust through a process of reputation analysis and explore how a process of reciprocation can update trust values in a positive manner. Allowing other agents in a distributed environment to influence the reputation of a particular agent, requires some form of reciprocation mechanism to be in place. A good reputation is built by the reciprocation of agents that are satisfied with a particular agent's performance. The satisfied agent reciprocates by increasing the agent that met its requirements' reputation.

Montaner, López and Lluís de la Rosa [10] look at the specific concept of defining trust through recommendation and thus also explore how to define trust in recommender agents. Recommender agents are the agents that give the recommendations in question. They focus on an opinion-based information filtering method. An agent that is unsure of a recommendation it receives, asks for the opinions of a set of agents it has defined as reliable. The key concept here is that the agents consulted are approached for an opinion on a recommendation that an agent is already in possession of and not a recommendation itself.

These are but a few of the trust models that have been proposed. It is clear that these models are varied, concentrating on different aspects of trust. Finding a commonality and structure among various trust models is often difficult if not impossible. This makes it difficult for an interested party to choose a trust model that best suits specific needs. This paper addresses this problem by defining a set of criteria anyone interested in trust model implementation can use in order to determine a trust model's efficiency. This set of criteria facilitate in identification of the core features of a trust model and the environment it works in.

3 CRITERIA FOR EVALUATION OF TRUST MODELS

Basic trust model architecture can be defined by four broad criteria, as defined by the author. These criteria include trust representation, initial trust, updating trust and trust evaluation. Trust representation looks at how a trust model represents trust-related data. Initial trust defines how a trust model obtains an initial trust value for a node it has previously not interacted with while trust update allows a trust model to dynamically update a trust value over time. Initial trust and updating trust are closely linked as usually the means in which initial trust is obtained, is usually carried through to the means in which it is updated. However, not all trust models follow this scheme. For instance, some trust models have no mechanism in place for establishing an initial trust value, others have none in place to update the trust values. Finally, trust evaluation looks at various

influencing factors on the trust evaluation process. Due to space constraints, trust evaluation is the only one of the four that is discussed in detail in this paper.

3.1 Trust representation

When looking at trust representation, it is important to note that we are looking at the way trust is represented from a holistic point of view. We are not interested in specific variables, their values and storage mechanisms. Rather we are looking at broader concepts that later influence specific trust representation, development and working thereof. Specific concepts include a trust outlook, passionate versus rational trust, centralized versus decentralized trust, trust versus distrust and trust scalability.

An agent's trust outlook defines an agent's predisposition to trust and the means in which it handles trust related data, and can be seen as either optimistic (expecting the best outcome), pessimistic (expecting the worst outcome) or pragmatic (balancing both optimistic and pessimistic). [2]. Passionate trust allows agents to be more flexible and to develop trust according to intangible principles that more closely emulate the formation of trust between humans. Rational agents are more prone to follow a defined set of rules that are expected to remain static and have the same result every time a trust analysis is done.

In centralised trust environments, all agents hold the same beliefs about all other agents. This belief is governed by a central authority. Decentralised trust is for environments where agents are allowed to leave and enter dynamically, making it difficult for a central authority to store all trust based information. In these types of environments, agents possess a more personal way of trust in that each agent has its own unique trust definitions for other agents. In many trust models a low trust value does not distinguish between distrust as a result of bad experience and distrust as a result of too little information. Explicit distrust parameters solve this uncertainty by storing the results of negative experience information. Finally, scalability considers various characteristics of a model in order to determine whether a model is scalable between small and larger environments.

3.2 Initial trust

Initial trust refers to the strategy a trust model adopts in order to obtain an initial trust value for another agent in the environment. There are several strategies that can be chosen and used. These include but are not limited to recommendation, reputation, observation, institution, collaboration, negotiation and experience [1], [3], [4], [9], [10]. All of these require that the model gather some form of information in order to establish a trust value before participating in an interaction with another agent. Initial trust is a means of establishing a trust value in order to interact with an agent that has previously not been encountered, before experiences, that can be judged, have been obtained. The defined methods of building this form of trust are based on those found in human psychology. For instance, reputation based trust is based on the human tendency to trust, based simply on hearsay and reputation.

3.3 Updating trust

Due to dynamic trust environments influencing agents and trust contexts, a means of updating trust is vital. This allows an agent to change a trust value over time in order to keep up with changing environmental and situational factors that rapid changes in technology and development are prone to cause. Agents are, thus, able to protect themselves from other agents that used to be trustworthy but became malicious over time. Often trust is updated using the same mechanisms that were used to define initial trust though there are a few additional factors that need to be taken into consideration. These are the influences of direct experience, feedback and transaction analysis. Direct experiences and feedback are merged along with the methods of establishing initial trust in order to obtain a more personal evaluation of trust.

3.4 Trust evaluation

In order to successfully update trust, a trust model needs a means of evaluating the information it has gathered. Many trust models rely on categorisation in order to limit the trust given to an interaction. This trust categorisation is used to evaluate an interaction and occurs in many various ways. Various trust models rely on the means in which they establish initial trust and update trust in order to evaluate trust and form various categories. However, there are factors other than the ones that are used to form trust that influence the success of interactions. Good trust models take these factors into consideration when evaluating the result of an interaction. These factors include trust context and risk. When taking these factors into consideration, a trust model often is required to do a more detailed analysis of trust. Trust models take two general approaches towards the detail to which trust is evaluated: that of approximate or dynamic evaluation. All of these concepts are important to consider when evaluating a trust model and are discussed in the sections that follow.

3.4.1 Trust categorisation

Trust categories allow for an agent to specify the specific context in which a certain relationship is given trust. For instance, certain agents may be trusted to forward data but may not be trusted to analyze the data [11]. The means in which categorisation occurs, influences the trust assigned to another agent. Two main means of categorisation have been identified by Li, Valacich and Hess namely Reputation (second hand knowledge) and stereotyping [12].

Reputation allows an agent to categorize other agents as a direct result of reputation information it receives about other agents. Various reputation-based models have various ways of implementing this form of categorisation and various actual categories into which these agents can fall. For instance, reputation can be gathered through recommendations, or through observation of an environment. Section 4 gives an example of one such model and the categories into which the model places other agents.

Stereotyping allows for agents to make assumptions about other agents depending on which category an agent falls into [13]. For instance, agents can be categorized according to which organization they belong to, the rights they possess, the roles they play and even the policies they are required to adhere to. Each category is in possession of rather specific privileges and rights associated with it [14]. For instance an agent assigned an administrative role will be given access to far more information than an agent simply assigned a client role.

The means in which this categorisation occurs influences a model's efficiency on various environments. Stereotyping works very well in environments where specific categories can be explicitly defined and tend to remain static over time. This means of categorisation allows for faster analysis than that of simple reputation because an agent can simply ask for category information and make assumptions based on this. Forming categories from reputation information requires a higher processing overhead but is more effective when no static explicitly defined categories exist, allowing agents to create their own categories as they are required. It is also possible to leave specific categories for reputation information undefined and allow the reputation value for an agent to be a category on its own.

3.4.2 Context

Trust is entirely based on situation. An agent needs to take into consideration situational constraints before it chooses to participate in a trust-based interaction. Such constraints include capability, need for an interaction and state of the environment [3]. Often the environment changes due to extenuating circumstances, such as a crash of a critical machine or hacker activity. Agents need to be able to detect such changes in the system and take alternative action, especially if such unexpected changes have influenced a critical part of the system as a whole. Shrobe, Doyle and Szolovitz[15] recommend that systems have a means of determining to what degree various agents

can be trusted so that agents may know which contingencies can be taken and which other agents can be trusted with sensitive information should a critical node in the environment be compromised.

A contextual factor that may influence the formation of trust is intention. The reason an agent seeks to establish a trust relationship is a clear indicator of a need that has been expressed. It is also the determining factor as to which information will be shared and which will be withheld. The context a transaction occurs in is also critical when evaluating the feedback that is received. For instance, the size of a transaction is indicative of the effort that was required in order to successfully complete the transaction. Small transactions carry lower risk than large transactions and so success in a small transaction should have a smaller influence on trust than one on a large interaction.

Contexts include both transactional context as well as environmental context. Transactional context include size, category and time of a transaction. Environmental contexts are more concerned with the state of the environment at the time of a transaction. Such contexts include which agents were running and which were not, suspicious increase in activity, network overload and addition of new agents [4]. Context is, hence, a means of controlling various interactions and it is important to determine whether a trust model takes this into consideration. Trust model implementations that neglect to take context into consideration, result in poor trust evaluations due to the depth to which context influences interactions. When choosing a trust model implementation it is also important to note what type of contexts are taken into consideration. In order to find a trust model that works optimally for a certain business environment, it is important that the type of context that is taken into consideration be the same as the contexts that most influence the business itself. For instance, a business with high risks needs to find a trust model that considers the risk of interactions before assigning trust values.

3.4.3 Risk

All trust relationships carry some form of risk factor with them. This applies not only to business context but any context where an exchange of information or service is required. In order to successfully handle this factor, risk needs to be assimilated into the decision-making process and accepted as inevitability. Helpful ways of dealing with risk is by having fallback mechanisms to do some form of damage control should the worst case scenario actually come about. Knowledge of risk allows for making plans that take this risk factor into account and so this factor can by no means be ignored [1]. A means of controlling the risk encountered in an interaction is by placing constraints on both the truster and the trustee while requiring the interaction to take place within these predefined constraints.

The very presence of risk in trust relationships has both the potential to positively and negatively influence trust levels. Successful completion of an interaction that is laced with risk boosts the trust level. Unsuccessful completion can seriously cause trust value to drop, especially if the risk was large and serious harm has resulted from the interaction.

It is important to note that risk is not the same as uncertainty and ignorance. It situations of risk, the various states of the environment and their probable influences on the interaction are known. In uncertainty the probable influences of the states are not known while in ignorance an agent may be unaware of even the existence of the states that could influence an interaction [1]. This brings to fore the fact that the very existence of uncertainty and ignorance is a risk to the system. An agent can work under any of these three states depending on the knowledge it had access to prior to encountering an interaction with another agent whose trustworthiness is in question.

A means of determining and handling the risk inherent in forming trust relationships is a vital component in a trust model. There is a trade off between the risk a trust model takes during interactions and the processing required analyzing another agent. The less detailed the analysis the larger the risk will be which leads us to the concept of dynamic versus approximate evaluation.

3.4.4 Dynamic versus Approximate evaluation

When implementing trust architecture it is important to decide on the means in which one wishes one's trust evaluation to occur. When participating in trust evaluation there is a clear trade off between the accuracy of trust evaluation and the processing power required to do a trust evaluation. In order to have an accurate trust evaluation a more dynamic approach is taken that continually incorporates changes in the environment and agent's interactions into trust evaluation. This is clearly a time-costly procedure. In order to save on processing and time, an agent can choose to do a more approximate evaluation of trust. This alternately carries the risk of a trust evaluation being inaccurate [4].

These four broad criteria categories have been proposed in order to ease analysis of currently proposed trust models. The next section demonstrates how this analysis process works for trust representation. An existing trust model is chosen and analysed using various points within the trust representation criteria category.

4 EXAMPLE ANALYSIS OF TRUST EVALUATION

The trust model chosen in order to demonstrate a sample analysis using trust representation is Abdul-Rahman and Hailes' Trust-Reputation model [16]. This model was chosen due to its relative simplicity. This model determines the trustworthiness of other agents based on collected statistics that include direct experiences and recommendations.

A subset of these direct experiences and recommendations is summarized in order to obtain a trust value. Experiences are recorded into two separate sets in order to be able to differentiate those that are a result of direct trust and those that are linked to recommendation. This way an agent is able to keep track of the direct trust it has in others as well as the trust level it has in recommendations from other agents.

In order to obtain a direct trust value for a particular agent in a particular context, this model relies on a basic system of counters. For every agent within a specific context, an agent possesses four counters. These counters are for varying trust degrees. The four counters this model makes use of are counters or very good, good, bad and very bad. Hence, these counters represent various trust levels namely very trustworthy, trustworthy, untrustworthy and very untrustworthy respectively. These counters are incremented with direct experiences an agent has. The trust model runs a max function on these four counters that return the counter that has the largest value for the specific agent in a specific context. The trust counter with the largest value indicates the trust level that is to be assigned.

Trust values that agents receive as recommendations rely on a semantic closeness value for analysis. This semantic closeness value determines how closely a recommender agent's perception of trust with another agent resembles that of the agent seeking a recommendation. Because trust is a subjective concept, it is logical to assume that perception of trust will differ among different agents. What one agent may define as trustworthy could be seen as untrustworthy by another agent based simply on differing perceptions. Thus, agents seeking recommendations are allowed to adjust recommendations it receives according to their own perceptions.

In order to accomplish this, an agent needs to obtain an adjustment value. In order to obtain this adjustment value, an agent compares its own trust evaluation result for a particular context with the trust evaluation result of the recommender agent in the same context. If the trust evaluation result differs, the agent creates an adjustment value for recommendations coming from that particular recommender in that particular context.

For example, agent A is looking for an adjustment value for recommender B. Agent A knows that the trust value it has for agent D is 't' (trustworthy) in context C. A receives information from B that B's trust value for D in context C is 'vt' (very trustworthy). In other words, A's value for agent D in the same context as B's value for the same agent is one level lower than B's. The

adjustment value that A obtains will be -1. This value is then used to lower the trust value of all recommendations coming from agent B by 1 in order to more closely represent A's own perceptions.

This trust model is analysed using the concepts discussed under the trust representation section as follows.

Categorisation: The type of categorisation this model uses is the reputation based categorisation. This trust model creates its own rather unique categorisation system as a result. Agents are not only identified, but interactions with them are categorized by the context in which they occur. The contexts are left open to definition and any required context can be chosen. Every context with a particular agent has four counters associated with it. The highest of these four counters indicates the trust level associated with the particular context and agent. Once trust evaluation of the counters occurs, the resulting agent's trust level can fall into any of five main categories that influence the trust given the interaction. These are 'vt' very trustworthy, 't' trustworthy, 'u' untrustworthy, 'vu' very untrustworthy and uncertainty which is a mixture of a trustworthy and untrustworthy value. Uncertainty is achieved when there is more than one maximum value for the four types of possible experience counters. The uncertainty assigned can lean towards positive trust, negative trust or remain neutral depending on where the uncertainty lies. If there is uncertainty between very good and good trust levels, then it is a positive uncertainty. If there is uncertainty between very bad and bad trust levels, then it is a negative uncertainty. All other combinations result in neutral uncertainty.

Context: This model specifically takes context into consideration when dealing with other agents. In fact, context is seen as so important that the same agent will have varying trust values in different contexts. This model requires an agent to save trust levels in agent-context pairs so that when trust is determined it is not only the particular agent, but the context as well that is looked up. The context is left undefined so that various forms of contexts can be chosen by anyone wishing to implement the particular model.

Risk: This model has no explicit consideration of risk but contains several implicit risk management mechanisms. This is explicitly defined as a reputation-based model. By definition, such models usually rely on second hand information in order to determine a trust value for another agent. This method inherently carries the risk of receiving false information from another. This risk is addressed by allowing agents to incorporate both direct as well as indirect information together. Agents are also required to analyse the worth of another agents recommendations by comparing a decision the recommender has made about another agent in a given context with the decision the agent itself has made about the same other agent in the same context. The result of this analysis is an adjustment value that an agent uses to adjust all recommendations coming from that specific recommender. Another means of handling risk is by allowing an agent to assign an uncertainty trust level if there is not enough information or if information the agent has gathered is contradictory. Experiences increment the counters associated with a particular agent in a particular context with the result of the experience. For instance, good experiences increment the good counter mentioned above. This continual process of updating the value allows for changes in the system to be echoed by changes in trust thus lowering the risk of having a trusted agent suddenly become malicious.

Dynamic versus Approximate Evaluation: This is a dynamic approach allowing an agent to record a set of experiences that it later uses, in order to determine a trust value. Experiences are updated and the updates influence further trust evaluation for agents in specific contexts. Agents gather recommendations from other agents and merge them in order to obtain a global, more specific, analysis. As more experiences are stored, the evaluation process becomes longer and the danger of running out of space when dealing with large number of agents and interactions exists.

5 DISCUSSION

This paper addresses the problem of analysing various trust models in order to determine the value of a trust model and pinpoint issues that have not been addressed. Four main categories of criteria have been identified by the author. These categories define the main features any good trust model is required to have. The main categories identified are trust representation, initial trust, updating trust and trust evaluation.

Due to space constraints, only one of the four criteria categories has been discussed in detail. The chosen category is that of trust evaluation. Trust representation has already been discussed in another paper submitted for review [17]. Initial trust and updating trust were not discussed due to their length and space constraints. The first three categories, therefore, have not been addressed in this paper in detail. Factors influencing the means in which trust is evaluated that have been identified and discussed in this paper include trust categorisation, trust context, risk and whether the trust evaluation process is dynamic or approximate.

6 CONCLUSION

This paper introduced and discussed the concept of a set of criteria that is to be used for the evaluation of trust models. These criteria are intended to be a guideline to trust model evaluation in order to identify the worth of a particular trust model as well as the areas in which a trust model lacks attention. In the same way that they can be used to evaluate a currently implemented trust model, they can also be used as a guide for factors and issues to take into consideration for future trust model implementations.

Using these criteria, one is able to identify how a trust model addresses certain issues and also which issues have not been addressed. This is important knowledge to have when considering choosing a particular trust model for implementation and can also be used to guide future improvements on trust model architectures.

Abdul-Rahman and Hailes' Trust-Reputation model was taken as an example and analysed using the factors identified within the trust evaluation criteria category. It is important to realize that this criteria are not necessarily all the possible defined criteria that can be taken into consideration. They are based on 'known' issues and known implementations and it is possible to expand them in future work. Future work also includes the development of a measurement mechanism in order to score the degree to which a trust model addresses the issues identified.

7 ACKNOWLEDGEMENTS

This research is funded through the Centre of Excellence in Teletraffic Engineering for the Information Society (CeTEIS), Telkom SA Limited. Any opinion, findings and conclusions or recommendations expressed in this material are those of the author(s) and therefore Telkom does not accept any liability thereto.

8 REFERENCES

[1] Marsh, S.P. Formalising Trust as a Computational Concept. In *Dissertation for the Department of Computing Science and Mathematics*, University of Stirling. 1994.

[2] Abdul Jonker C.M. & Treur J. 1999. Formal Analysis of Models for the Dynamics of Trust based on Experiences. In *Modelling Autonomous Agents in a Multi-Agent World*, pp 221-231. 1999.

[3] Wang, Y. & Vassileva, J. Bayesian Network-Based Trust Model. In *Proceedings of Web Intelligence, 2004*. WI 2004. IEEE/WIC?ACM International Conference on 20-24 Sept 2004. pp 341-348. ISSN: 0-7695-2100-2

[4] Li. X. & Liu, L. PeerTrust: Supporting Reputation-Based Trust for peer-to-Peer Electronic Communities. *In IEEE Transactions on Knowledge and Data Engineering*, Vol. 16 No. 7

July 2004.

[5] Blaze, M, Feigenbaum, J, Lacy, J, Decentralized Trust Management, *sp*, In *IEEE Symposium on Security and Privacy, 1996.* p. 0164, 1996.

[6] Wen, W. & Mizoguchi, F. An Authorization-based Trust Model for Multi-agent Systems. 1999? http://www.istc.cnr.it/T3/download/aamas1999/Wen-Mizoguchi.pdf. Last Accessed: 23 April 2003.

[7] Nooteboom, B., (2002) Trust: Froms, Foundations, Functions, Failures, and Figures, Edward Elgar Publishing, Ltd. Cheltenham UK, Edward Elgar Publishing, Inc. Massachusettes, USA

[8] Golembiewski, Robert T., & McConkie, Mark. 1975. The Centrality of Interpersonal Trust in Group Processes. Chap. 7, pages 131–185 of: Cooper, Cary L. (ed), Theories of Group Processes. Wiley.

[9] Mui, L., Mohtashemi, M. & Halberstadt, A. A Computational Model of Trust and Reputation. In *Proceedings of the 35th Hawaii International Conference on System Sciences*. 2002

[10] Montaner, M., Lopez, B. & Lluis de la Rosa, J. Developing Trust in Recommender Agents. In *Proceedings of the First International Joint Conference on Autonomous and Multi Agent Systems* (AAMAS'02). Bologna (Italy) 2002.

[11] Pirzada, A.A. & McDonald, C. Establishing Trust in Pure Ad-hoc Networks. In *Research and Practice in Information Technology*. Vol. 26 V. Estivill-Castro, Ed. 2004.

[12] Li, X., Valacich, J.S. & Hess, T.J. Predicting User Trust in Information Systems: A Comparison of Competing Trust Models. *In Proceedings of the 37th Hawaii International Conference on Systems Sciences.* 2004.

[13]Khare, R., & Rifkin, A., Weaving a Web of Trust. In: *World Wide Journal*, Volume 2, Number 3, 1997, pp. 77-112.

[14] Shand, B., Dimmock, N. & Bacon, J. Trust for Ubiquitous, Transparent Collaboration. In *First IEEE Conference on Pervasive Computing and Communications.* Ft. Worth, Texas, USA. 2003.

[15]Shrobe, H., Doyle, J. & Szolovitz, P. Active Trust Management for Autonomous Adaptive Survivable Systems. In *Proposal to the Defense Advanced Research Projects Agency in response to BAA #00-15 "Information Assurance and Survivability (IA&S) of the Next Generation Information Ifrastructure (NGII)".* 1999.

[16] Abdul-Rahman, A. & Hailes, S. Relying on Trust To Find Reliable Information. In *Proceedings of DWACOS'99, Baden-Baden, Germany.*, 1999.

[17] Wojcik, M., Venter, H.S. & Eloff, J.H.P Trust Model Evaluation Criteria: A Detailed Analysis of Trust Representation. Submitted for review for SATNAC 2006