

A lightweight Model of Trust Propagation in a Multi-Client Network Environment. To what extent does Experience matter?

Marc Conrad, Tim French, Wei Huang
University of Luton, Park Square, LU1 3JU, United Kingdom

Introduction

Trust applied within Computing contexts is usually seen as comprising two distinct sub-areas of intellectual enquiry: namely *tangible* and *intangible* trust. In the context of computer security, the term trust is often used by academics and industrial practitioners alike as a convenient label for a surprisingly diverse set of enabling technological mediators, human stakeholder requirements and expectations. A number of large scale and small scale initiatives and groups have become active. The iTrust consortium for example (iTrust, 2005) has carried out valuable work in probing trust in a variety of E-service contexts. The recently established Oxford Institute for Internet Studies (<http://www.oii.ox.ac.uk>) has identified trust issues as an area of concern and has supported large scale consumer surveys to generate more empirical evidence concerning consumer trust formation in E-Service contexts. Emergent Grid and Web-Service E-Service architectures are being currently examined from a trust perspective by a variety of research groups (SECURE, 2001; Rana et al, 2004). Various commercial initiatives have attempted to support trust formation in B2C through the development and use of so-called trust signs and seals. For example the *Internet in Media Retail Group* (an industry based consortium of major UK retailers) has initiated the 'Internet is Safe' (ISIS) site accreditation initiative, designed to lower the trust barrier as between accredited on-line retailers and their customers through the deployment of the ISIS trust seals and related measures (IMRG, 2004). These, and the previous similar commercially directed trust accreditation initiatives indicate that E-Service providers implicitly recognise the key role of trust in mediating on-line shopping transactions. Thus, intangible trust can be considered to form a distinctive area of intellectual enquiry that is both highly relevant industrially and intellectually relevant to modern Computer Science as an academic discipline (French and Liu, 2005).

It is clear that a directed network of people connected by ratings or trust scores, together with a suitable propagation model has become a fundamental part of several highly successful E-commerce business models including E-Bay. As such, trust and distrust propagation across networks has emerged as a distinctive field of research in its own right (Guha et al, 2004). Previous work has sought to account for trust as an intangible aspect of B2C systems (Egger, 2004) in terms of high usability equating to high levels of trust (French and Liu, 2005). Furthermore, many have sought to construct and suggest the use of trusted XML (Extensible Markup Language) based architectural solutions to the issues of trusted Web and Grid services through the creation of a multi-layered platform neutral architecture mediated by standards such as SAML (Security Assertion Markup Language) and identity management supported by agents.

A number of trust rating systems that are in use are still in the process of being piloted. Aside from specialist models such as that used by E-Bay, the notion is to establish a web-of-trust so as to enable trust ratings to be assigned by one person to

another and from a person to a technical mediator. In some cases such systems are intended to be used person-to-person, in other cases the idea is to enable autonomic agents to establish and verify rating to proxy human identities and to mediators, e-commerce sites etc. The approach aims to mimic (in a fairly crude mechanistic form) the kinds of subjective assignments of trust or mistrust that human actors instinctively or consciously make, whilst engaging in various forms of E-service and E-platform transactions. With specific reference to the emergent semantic web for example, ontologies can be used to describe and express the degree of trust that an entity or person has in another person or entity. One example of an ongoing initiative being the FOAF („Friend of a Friend“) semantic web trust initiative (<http://trust.mindswap.org/>).

We seek to offer an alternative lightweight approach that seeks to mimic human trust formation in an entity to entity (client-server) network of computational nodes. Our motivation is to mimic well known successful commercial trust rating systems and to harness the aggregating power of these trust rating systems so as to solve the problem of trust management across heterogeneous distributed networks. As such we implicitly challenge the various initiatives offered by Web-Services standards groups and others who seek to build a complex multi-layered XML Web-Service based architecture to engender trust in distributed client server contexts. This is not to say our approach is antagonistic to these initiatives, rather it can be regarded as being complementary or even capable of being integrated within these heavyweight approaches.

The model that has been presented does not seek to address trusted identity and signature issues. These lie outside the present scope of the model. Our emphasis has been centered upon a definition that interprets trust as a mixture of prejudice, experience and hearsay. Hence we focus on a system of clients accessing a server where the clients are able to share information about the trustworthiness of the server.

The remainder of the paper is organized as follows. First we establish and evaluate the mathematical model that is used to simulate trust in Multi-Client systems. Following that we describe how the experiments made in this model show that the question raised in the title has a definitive answer: Under certain assumptions a Multi-Client system is best configured if ‘experience matters for 30%’.

The Mathematical Model

The model introduced here has been inspired by real world experience of human-human interaction. We model trust relationship in a grid or a network as a combination of the three main values that we call *prejudice*, *experience* and *hearsay*. These variables then compute a value *trust*. The basic formula used is

$$trust = selfConfidence * experience + (1 - selfConfidence) * hearsay \quad (1)$$

where *selfConfidence* is a well defined value between 0 and 1. We discuss the optimal choice of *selfConfidence* in the following section.

In our scenario a number of clients that have access to each other are making requests to a service. Every client maintains its own set of variables *prejudice*, *experience* and

hearsay for this server. For simplicity we assume that all variables are in the interval [0:1], where 0 indicates a negative attitude towards the service while 1 denotes full satisfaction. We will discuss these three variables and their interrelationships below.

Prejudice: This is used as the initial value of the other two variables *experience* and *hearsay*. As we will see, *experience* and *hearsay* are computed iteratively, that is *experience* is based on previous *experience* and *hearsay* is based on previous *experience* of other clients using this service. In an inherently trustworthy system (for instance in a grid where the assumption is that a server is dedicated to deliver the service, and failures happen only as a result of error conditions) the initial value of prejudice is equals 1, i.e. the client assumes a full trust towards the service. We will see that the impact of prejudice towards the trust of the client system towards the server is decreasing when the number of requests by the clients is increasing.

Experience: In our model we assume that the client is able to verify that a service was successful or not, i.e. the client is able to evaluate the quality of the service. This verification may be possible directly for problems in suitable complexity classes, for instance number factoring is known to be known a difficult problem that needs sophisticated approaches. However, if a ‘factoring service’ returns 2111 and 2143 as prime factors of 4544983 this result can be easily (i.e. in polynomial time) verified by computing $2111 * 2143$. In other cases the service may be evaluated via plausibility tests or verified via computed hash values etc. We call this the *immediateExperience* (again a value between 0 and 1 where 1 denotes maximal satisfaction) of a client request, and *experience* is calculated via the formula

$$experience := (immediateExperience + experience)/2$$

We observe here that the influence of a particular experience a client had with the server at the k th encounter decreases exponentially when k increases.

Hearsay: We assume that every client c is linked to a set R of other clients, that we call the referees of c (for a given service). The value *hearsay* is then computed as the average of trust of the referees of c , that means we set

$$hearsay := hearsay(c) = |R|^{-1} \sum_{r \in R} trust(r) \quad (2)$$

where $trust(r)$ is the trust that the client r has towards the service. Please note that $trust(r)$ is a variable that is updated whenever a client r makes a server request. It is not dynamically computed when accessed in order to avoid possibly infinite recursions as we cannot assume that the clients are organized in hierarchies, i.e. two clients can be referees to each other.

Experimentation and Results

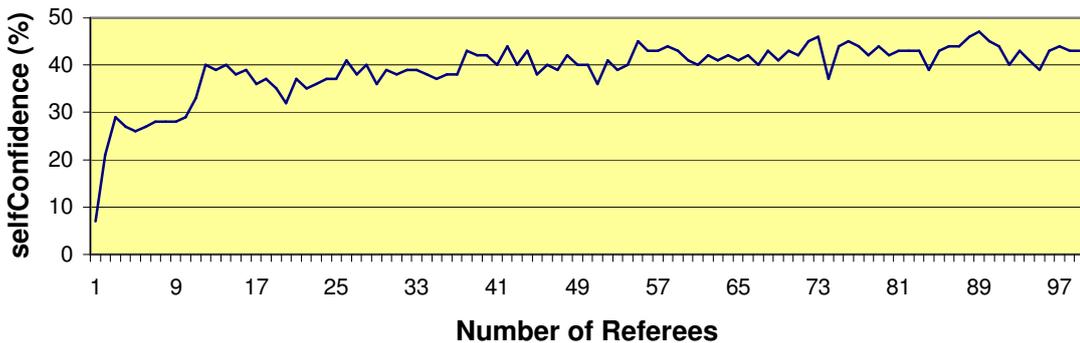
In order to identify an optimal value of *selfConfidence* in formula (1) we conducted a number of simulations. The code used for the simulations has been written in Java and is available from the authors upon request. To run these simulations we made the following assumptions:

- The server is prejudiced with a value of 1, that means that all clients initially trust the server ($trust = 1$).
- The return of the server is only pass or fail, i.e. the *immediateExperience* for every request is 0 or 1 (but not a value in between).
- The server fails with a probability of 5%. However the client wants a trust of 99%, that means a client stops making requests to the server if $trust < 0.99$.
- The metric to determine an optimal value of *selfConfidence* is given by the overall (i.e. system wide) number of unsuccessful client requests (#ucr) to the server.

The set of initial assumptions stated above reflects what may be a typical situation in a Multi-Client system. It is of course possible and a necessary part of ongoing and future work to seek to adjust these in a systematic manner and to observe the feasibility and applicability of the model described here under these different assumptions. However, this particular set has been selected on a rational basis as at least a starting point for further model simulations under a variety of conditions.

For determining the optimal value of *selfConfidence* we run a Monte-Carlo method with a random sample of client systems. This has been tested on client systems with k referees for each client with $1 < k < 99$. The findings suggest an interesting correlation

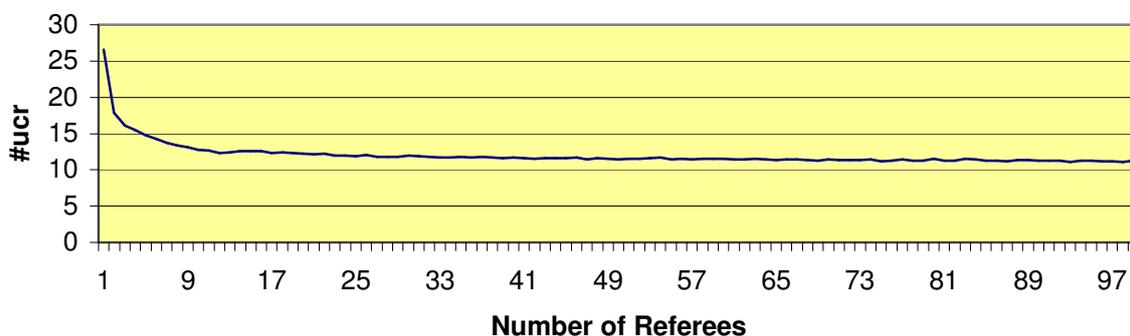
Figure 1: Optimal self confidence in relation to number of referees



between the optimal value of *selfConfidence* and the number of referees for each client (Figure 1): In fact the optimal *selfConfidence* is relatively stable at around 40% when the number of referees is greater than 15 and around 30% for values from 5 to 14.

In addition Figure 2 shows the absolute number of unsuccessful server requests (#ucr) in relation to the number of referees. This suggests that the number k of referees plays

Figure 2: Number of unsuccessful Server Requests against number of Referees



a crucial role for small values of k . However the change is less significant for larger values, say $k > 10$. From formula (2) we observe that when $k = |R|$ increases the overall performance of the implementation decreases (as for each trust computation more referees need to be checked), hence in our example system determined by the assumptions above we suggest the following values:

- Number of referees: $k = 10$
- *selfConfidence* = 30%

Conclusion

Previous research into trust issues has enhanced our understanding about trust antecedents and trust determinants in relation to intangible trust formation, mainly in B2C consumer and E-Service contexts. It is our contention that such ‘soft’ modeling approaches to trust can be leveraged so as to help solve the issues of trust as between computational entities in Web and Grid service contexts. The advantage of this approach is that it offers a relatively lightweight and transparent approach to trusted computation across network nodes as compared to existing initiatives that rely on multi-layered XML architectures. This is not to say that our approach can replace these initiatives as they embrace wider social and organizational aspects of trust (WS-Agreement) as well as the exchange of trusted virtual credentials and tokens (WS-Trust). Rather our aim is to suggest that mimicry of human trust formation by a light-touch approach can yield valuable insights into the propagation of trust across networks. Later, these insights can be harnessed and potentially integrated into existing mainstream approaches to Multi-Client architectures. Clearly, much further work is needed to validate and fine tune the model presented above but it is hoped that this initial paper will highlight the need to leverage previous research into human-computer intangible trust issues in client server contexts of use.

References

- Egger, F., (2003). *From Interactions to Transactions: designing the Trust Experience for B2C Electronic Commerce*, PhD Thesis, Department of Computer Science, Technical University Eindhoven.
- French, T., Liu, K., (2005). *Trust for E-commerce*, Procs. ALOIS*2005 3rd International Conference, Limerick University, Ireland, 15-16th March 2005, p. 99-113. ISBN 1-874653-79-8.
- Guha, R., Kumar, R., Raghavan, P., Tomkins, A., (2004). *Propagation of Trust and Distrust*, IBM Research Paper, available from: <http://www.tomkinshome.com/papers/trust/final/p423-guha.htm>
- IMRG White Paper: *Trust on-line: facilitating trust in on-line shops*, (2000-2004), IMRG (Internet Media Retail Group), available as a PDF download from: <http://www.imrg.org/8025696F004581B3/pages/imrg+Resources>
- iTrust 3rd International Conference on Trust Management, May 23-26th, 2005, see: <http://www.itrust.uoc.gr/prodshow.cfm>
- Rana, O., Moreau, L., Padget, J., (2004). *Trusted Grid Workflows: Assigning Reputation to Grid Service Providers*, ERCIM News, Special Theme: “Grids: the Next Generation”, No. 59, October 2004, 43-44.

- SECURE: *Secure Environments for Collaboration among Ubiquitous Roaming Entities*, (2001) IST Project: IST-2001-32486, Department of Science University College Dublin, available from: http://www.dsg.cs.tcd.ie/dynamic/?category_id=-30