ISSN : 0974 - 7435 Volume 8 Issue 3

BioTechnology
An Indian Journal

FULL PAPER

BTAIJ, 8(3), 2013 [347-351]

Study of the risk assessment module

Cao Yonghui
School of Economics & Management, Henan Institute of Science and Technology, (CHINA)
School of Management, Zhejiang University, (CHINA)
E-mail: caoyonghui2000@126.com

ABSTRACT

Just as the RSM was an instantiation of Interpersonal Trust, the Risk Assessment module (RAM) implemented System Trust. In this paper, the RAM monitored globally available information, in the form of reports from the KMS. These reports were aggregated to determine the general uncertainty in the network. This process gave a node the general impression of the network's "trust state." This was an expression of how risky an action was likely to be, given the current state of trust events in the network. Simplistically, this trust state can be phrased as "if other people are having success then I'm more likely to give it a try."

KEYWORDS

Risk assessment module;
Trust types;
Trust thresholds.

INTRODUCTION

Trust, and more importantly decisions on trustworthiness, is omnipresent in life. Luhmann's sociological approach[1] considered trust as "a means for reducing the complexity in society." This complexity was created as individuals interacted using their own perceptions, motivations, and goals. Solomon and Flores[2] contended that "trust forms the foundation, or the dynamic precondition, for any free enterprise society." They pointed out that what constituted freedom was the right to make promises and, more importantly, the responsibility for fulfilling them. Trust, therefore, was the basic underpinning of a cooperative environment. Trust was not an inherited trait but was learned as a member of the environment interacted with others. Another applicable definition of trust was provided by Gambetta[3].

"…trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent will perform a particular action, both before [we] can monitor such action (or independently of his capacity of ever to be able to monitor it) and in a context in which it affects [our] own action."

Humans usually based the decision to trust on historical evidence that led them to predict another person or entities' future behavior[4]. When this prediction was shown to be incorrect, the other person was trusted less, if at all. Rather than accept a philosophical betrayal, because "trust can only concern that which one person can rightly demand of another"[5], humans acknowledged the presence of selfishness in their environment[6] and took steps to avoid being victimized by self-centered peers. Any declaration of another's selfishness was dependent on establishing the context of the trust evaluation.

Time and context were two characteristics of the

FULL PAPER

multi-dimensional nature of trust. The time aspect showed that trust was dynamic; a disreputable person could redeem himself through honest actions and a trusted person could become less reputable if he demonstrated deceit. Context was the situation in which trust was being considered. An example of context was that Alice may trust Bob to order wine at dinner but wouldn't trust him to fix her car.

Trust could be transitive, as shown in Figure 1. If Alice trusted Bob to pick wine and Bob trusted Charles to pick wine, Alice might reasonably trust Charles in wine selection if she were applying transitive trust. Alice could also constrain this trust by context. The constraint meant that, although Bob might trust Charles to split the bill fairly, Alice might have been willing to risk Charles' wine choice but might not be expected to trust the way he divided the check.

Alice might choose to constrain her trust through association, illustrated on the right side of Figure 1. This type of trust required Alice to gauge the extent she trusted Bob before asking his opinion on Carl's trustworthiness. Bob would reply with a qualified expression of his estimate of Carl's trustworthiness. Once she had established her trust in Bob and his trust in Carl, Alice combined both trust levels to create her own initial impression of Carl's trustworthiness. Alice's guarded trust or cynicism allowed trust to be expressed in a continuous, rather than discrete, manner as it was in sociological settings.

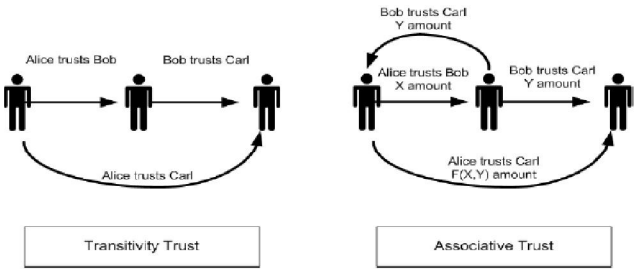

Figure 1 : Transitive and associative trust

Expressing trust in continuous terms qualified trust in terms of context (e.g., Alice trusted Bob's taste in wine) or acceptance of risk (e.g., since the bill was only $5, Alice was willing to see how Charles split the check). Individuals evaluated evidence of their peers' behavior, forming a perception of behavior through risking betrayal with each interaction. The means of determining trust was complicated by numerous definitions and applications of trust.

TRUST TYPES

Given the many, sometimes contradictory definitions of trust, McKnight and Chevrany[7] attempted to describe a framework that provided a taxonomy of three types of trust. From this taxonomy (shown in Figure 2), they were able to quantify and generalize the process an individual used to influence their behavior. Starting from the bottom of the figure, this model shows how the trust types combine with trust beliefs and are adjusted by trust intentions before becoming behavior; the expression of the trust decision.

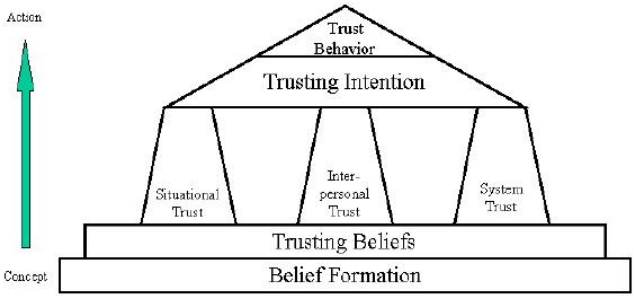

Figure 2 : Trust constructs

System trust

System Trust was the extent to which an individual placed trust in the environment around them. In a personal sense, this type of trust reflected a person's feeling of safety in their current location or present situation (e.g., Alice always locked her car doors when she drove through the downtown area.) System trust was built from both structural assurances and situational norms. The individual's belief that the system's rules and regulations would protect them was an example of structural assurance. Similarly, if a user's past experience was that a certain area was risky, the situational norm prompted his System Trust to provide appropriate protection.

Interpersonal trust

Interpersonal Trust was user centric and described an individual's general willingness to extend trust across a broad range of situations to any number of people. This type of trust, also called Dispositional Trust, formed the basis of an individual's approach to interaction. It demonstrated an expectation of other people once their

trustworthiness had been evaluated. Interpersonal trust was built from experience, either referred from other trusted individuals or from direct contact with the person in question. This was modified by a trait that McKnight and Cheverny call Trusting Beliefs, reflecting the general tendencies people had toward extending trust. Some people were trusting, believing in the goodwill of their fellow man. Other individuals were more cynical, requiring others to demonstrate their trustworthiness before risking interaction.

Situational trust

Situational Trust described the degree of trust that an individual was prepared to trust any other person in a given situation. This trust was formed upon the intention to extend trust in a particular situation, regardless of what the person knew or did not know about the other party in the situation. It was suggested that this type of trust occurred when the trusting party stood to gain with very little attendant risk. Situational trust was different than System trust because there was no implied structural or system safeguard. It was, in short, an individually conceived situational strategy and did not involve an evaluation of the trustworthiness of the other party.

THE RISK ASSESSMENT MODULE

Just as the RSM was an instantiation of Interpersonal Trust, the Risk Assessment module (RAM) implemented System Trust. The RAM monitored globally available information, in the form of reports from the KMS. These reports were aggregated to determine the general uncertainty in the network. This process gave a node the general impression of the network's "trust state." This was an expression of how risky an action was likely to be, given the current state of trust events in the network. Simplistically, this trust state can be phrased as "if other people are having success then I'm more likely to give it a try."

The original system design for the RAM had specified the use of an algorithm that constructed a decision surface[8]. The surface was calculated using probabilistic variables that expressed the expected gain and willingness to risk for an individual. These variables were set arbitrarily, instead of quantitatively or even heuristically. Because of this perceived flaw, Jøsang's method was not implemented in the proof of concept system.

The SECURE project[9] provided the following definitions:

- *Risk* describes situations where one is unsure of the outcome but the odds of success or failure are known.
- *Uncertainty* applies to situations where one is unsure of the outcome and the odds are unknown.

Using this definition, the TMS estimated Uncertainty instead of Risk, although the remainder of this document will use the terms interchangeably. The decision to use an uncertainty estimate to adjust a node's trust thresholds was recognition of the arbitrariness of attempting to define the world in terms of cost-benefit or payoff rather than in view of expected success or failure.

Uncertainty was calculated using global trust information from the KMS and first hand observations. In other words, each user approximated the risk of his local network by listening to the sources that he trusted implicitly. By monitoring the trend in reports and complaints, the user adjusted his trust and distrust thresholds to protect himself.

Because risk trends changed slower than reputation, the Global Risk Index (*GRI*) was calculated using a third order filter, shown in Equation 1. The third order filter was selected over other methods through testing. First order filters were too reactive to changes in environmental conditions, as discussed in our previous work[10]. Second order filters were better but still failed to provide the smooth trend line that described sociological conditioning to a risky environment. Equation 1 applied weights to the current FI and previous inputs before computing the new *GRI*[11].

$$\alpha = 0.35; \beta = 0.25; \gamma = 0.25; \delta = 0.15$$

$$GRI_t = (\alpha * FI_1) + (\beta * FI_2) + (\gamma * FI_3) + (\delta * FI_{t-1}) \quad \textbf{(1)}$$

This newly calculated *GRI* was then used to calculate the relative change in trust in the local network, shown in Equation 2. Here the default distrust threshold (*TD*) was modified by the current *GRI* to arrive at an operational distrust threshold (τD).

$$\tau_D = T_D - (GRI_t * T_D) \quad \textbf{(2)}$$

This equation had the effect of increasing the distrust threshold (along the y-axis of the threshold graph)

but not allowing the threshold to relax or decrease. The decision was taken to avoid adjusting the trust threshold, to prevent self-isolation. In essence, the risk assessment carries a grudge – even if the user moves to a safer neighborhood.

TRUST THRESHOLDS

Once a node selected a prospective peer, calculated that peer's reputation, and made a general assessment of risk, it needed to combine these into an evaluation to produce a trust or, in the case of a resource provider, an access control decision. This decision was accomplished by comparing the reputation to the risk-adjusted trust threshold.

Marsh[12] expressed the "cooperative threshold" in terms of expectations. A user calculated a threshold for each associate based on the perceived risk of the transaction and the perception of the associate's competence to complete the transaction. These context- sensitive perceptions are then tempered with the overall experience with that user to produce a threshold, which was applied for that specific transaction.

This approach displayed the common flaw of relying on expectation. Although expectations could be used in a logical or behavioral system, an individual's expectations were impossible to use in a quantitative system. Marsh's work (and those of the researchers who followed him) also failed to discuss a user's thresholds when they joined the network. Researchers implemented an initial state and analyzed how prevailing trust conditions acted to adjust these settings. Setting expectations remained a heuristic process and was unsuitable for nodes interacting with new and unfamiliar associates.

In the TMS, every user had two trust thresholds, as shown in Figure 3. Since reputations were expressed in values in the range of [-1,1], a user evaluated the reputations of prospective peers against these thresholds. One was a positive threshold, above which a user extended trust. The other was a negative threshold, below which a user withdrew trust. Between these two thresholds was a continuous range of trustworthiness. Reputation values varied within this "trust zone" based on interactions and environmental conditions.

In this research, therefore, the TMS made initial estimates based on the trust profiles discussed. These estimates were quantified as shown in TABLE 1. It was recognized that these estimates needed to allow a new user to meet and trust associates while, at the same time, provide a reasonable level of protection. Once a user had began to interact with other network members, the TMS adjusted the initial threshold values to protect the user. Because the TMS proved to be responsive to network conditions, the reliance on heuristically set initial values was not deemed a significant risk.

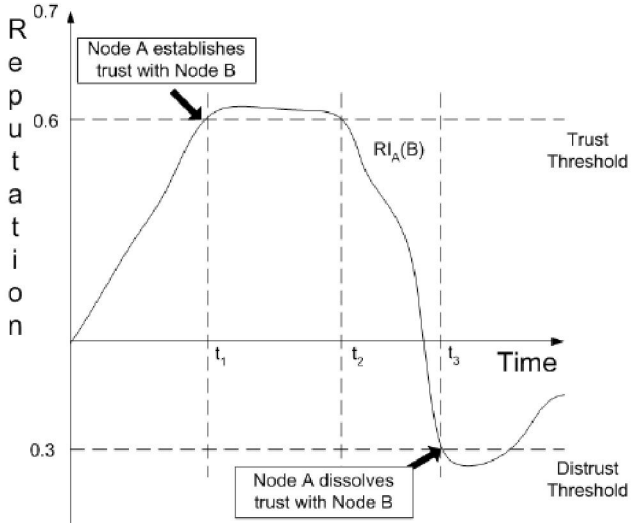

Figure 3 : Examples of trust threshold use

TABLE 1 : Example Initialization Values Based on Trust Profiles

Trust Profile	Trust Threshold	Distrust Threshold	Risk Constraint	Reputation Constraint
Altruistic	-0.99	-1	None	None
Forgiving	0.6	0.3	None	None
Cynical	0.7	0.4	Rising Only	Rising Only
Distrusting	NA	NA	None	None

A user established a trust threshold based on the selected trust profile, a shown in TABLE 1. Given that the system explicitly revoked the identity of any user with an RI=-1 and that users joined the network with an RI=0, the following provide a practical example to the use of trust thresholds in reputation-based systems. An altruistic user trusted a peer with an RI>-1, enabling any user that is allowed in the network the ability to establish trust with it. A forgiving user trusted any peer with an RI≥0.6, facilitating connectivity with new users and any existing user that had demonstrated desirable performance. Cynical users required a peer to have an RI≥0.7, indicating that a user had a demonstrated positive behavior history. New users or users working to

rehabilitate their reputations were not extended trust by cynical users. Note that while the definition of the Cynical trust profile stated that a Cynical user would not allow rehabilitation; in reality the system allowed a user to "start again" once their reputation crossed the X-axis in the positive direction. Distrusting users discounted trust and reputation, choosing to rely on MAC rules to allow access.

REFERENCES

[1] N.Luhmann; Trust and Power, Wiley, **(1979)**.

[2] R.Solomon, F.Flores; Building Trust. New York, NY, Oxford University Press, **(2001)**.

[3] D.Gambetta; Can we trust trust? Trust, Making and breaking cooperative relations, electronic edition. D. Gambetta, Univ. of Oxford: Ch 13, 213-237 **(1988)**.

[4] K.Aberer, Z.Despotovic; Managing trust in a peer-2-peer information system. Proceedings of the 10th International Conference on Information and Knowledge Management, Atlanta, GA, 310-317 **(2001)**.

[5] L.Hertzberg; On the Attitude of Trust. Inquiry, **31(3)**, 319 **(1988)**.

[6] P.Michiardi, R.Molva; Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks. Proceedings of the European Wireless Conference (EW2002), Florence, IT, 1-6 **(2002b)**.

[7] D.McKnight, N.Chervany; The Meanings of Trust. Technical Report, Carlson School of Management, University of Minnesota, **(1996)**.

[8] A.Jøsang, S.L.Presti; Analysing the Relationship between Risk and Trust. Proceedings of the 2nd International Conference in Trust Management (iTrust 2004), Oxford, UK, 29 March-1 April 2004, 135-145 **(2004)**.

[9] N.Dimmock, J.Bacon et al.; Risk Models for Trust-Based Access Control. Proceedings of the Third International Conference in Trust Management (iTrust 2005), Paris, FR, 23-26 May 2005, 364-371 **(2005)**.

[10] W.J.Adams, G.C.Hadjichristofi et al.; Calculating a Node's Reputation in a Mobile Ad-Hoc Network. Proceedings of the 24th IEEE International Performance Computing and Communications Conference (IPCCC 2005), Phoenix, AZ, 6-9 April 2005, 303-307 **(2005)**.

[11] R.Jain; The Art of Computer Systems Performance Analysis. New York, NY, John Wiley&Sons, **(1991)**.

[12] S.Marsh; Formalising Trust as a Computational Concept, Ph.D. Dissertation, Department of Mathematics and Computer Science, University of Stirling, **(1994)**.