ISSN : 0974 - 7435 Volume 8 Issue 3

BioTechnology
An Indian Journal

FULL PAPER

BTAIJ, 8(3), 2013 [352-356]

Study of the reputation scaling module

Jiang He

Department of Mathematics, Henan Institute of Science and Technology, Xinxiang, 453003, (R.CHINA)

ABSTRACT

The RSM (Reputation Scaling Module) was the heart of the TMS (Trust Management System). The RSM was responsible for accepting an associate's behavior history and calculating a RI (Reputation Index). The RI was a weighted estimation of the associate's trustworthiness and formed the basis for the TMS's trust decision. Without the RSM, the TMS would not have had the ability to process an associate's behavior history and, thus, have been unable to make any sort of trustworthiness decision. This paper explains the basic trust model that the RSM implemented and describes the method of how behavior observations were transformed into weighted FIs.

KEYWORDS

Reputation scaling module,
Trust types;
Trust management system.

INTRODUCTION

Trust, and more importantly decisions on trustworthiness, is omnipresent in life. Luhmann's sociological approach 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[1] 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 :

"…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[2]. 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" (Hertzberg 1988), humans acknowledged the presence of selfishness in their environment[3] 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 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 dem-

onstrated 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.

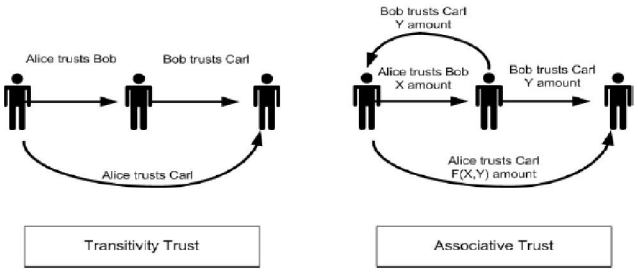

Figure 1 : Transitive and associative trust

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[4] 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.

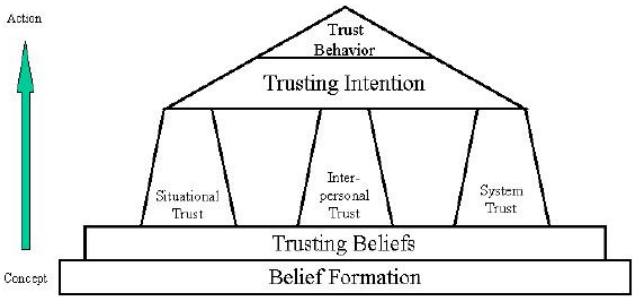

Figure 2 : Trust constructs

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 REPUTATION SCALING MODULE

The RSM was the heart of the TMS. The RSM was responsible for accepting an associate's behavior history and calculating a RI. The RI was a weighted estimation of the associate's trustworthiness and formed the basis for the TMS's trust decision. Without the RSM, the TMS would not have had the ability to process an associate's behavior history and, thus, have been unable to make any sort of trustworthiness decision.

The remainder of this section explains the basic trust model that the RSM implemented. The section then describes the method of how behavior observations were transformed into weighted FIs. The subsequent section explains the process by which FIs were "aged" through a series of weighted windows in the 3Win algorithm. Finally, the RI is defined in terms of a quantitative assessment of an associate's trustworthiness.

The RSM was the processing module that processed feedback to calculate a usable RI for its peers. The TMS implemented an Interpersonal Trust model[5] to represent the reputations that were compiled by a node on each of its peers. This trust type was node specific, so that the trust of one node to another was associative and not transitive. The following list summarizes the properties of the system's trust model:

a Trust was independent, subjective, and unidirectional, such that different nodes calculated different reputation values for the same observed node.

b Trust had positive and negative degrees of trustworthiness. Trust was expressed in continuous values that represented the range of reputation between untrustworthy (negative reputation) and trustworthy (positive reputation), as in Marsh.

c Trust was based on experiences and observations between individuals.

d Trust information was exchanged between nodes as performance observations and reports, as described below.

e Trust was dynamic and was modified, in a positive or negative direction, based on new observations and reports.

The design of the RSM required an examination of other reputation management systems. The requirements analysis indicated that the TMS needed to exchange and process evidence of behavior to produce a usable RI. The importance of the evidence was to justify how a node arrived at a reputation value for its peer. The same evidence was also used to provide non-reputable behavior history referrals to peers as they encountered nodes they met in the network and wished to assess the trustworthiness.

The system denoted the reputation Alice maintained of Bob as $RI_A(B)$. The RI was represented by number values in the range [-1, 1]. This value represented the trust Alice placed in Bob; the higher the number, the more trust was imparted. This number was never stored. It was always recalculated with the latest information. Peers viewed a user with a reputation of –1 as completely untrustworthy. Peers viewed a user with a reputation of +1 as completely trustworthy. The notion of "completely" in terms of trust was a theoretical limit; in practice the only peer that was completely trusted was the KMS.

Peers viewed users that they had no information about with a reputation value of 0. Liu and Issarny[6] pointed out that this assignment made no attempt to differentiate between newcomers, strangers, users that had not participated (freeloaders), or users whose reputations had been calculated to be 0. Zero was consid-

ered a neutral value as it gave a new user a basic reputation to start with while limiting the impact strangers, freeloaders, and active users with low reputations had on the network.The RI of 0 implied that the user needed more information before making a decision, rather than implying trust or distrust.

Although the RSM used behavior grading from a variety of sources, the TMS required the RSM to differentiate between reports and observations. The former were provided by the KMS as described in Section 0 and indicated an action taken to establish or dissolve a trust relationship. Observations dealt with the performance of TPs and were a function of the network monitor that supports the reputation management system. A node observed the performance of its TPs and Friends. It periodically generated positive or negative FIs and passed them to its TPs. The generation of a negative observation did not imply immediate dissolution of the association.

The TMS implemented a system of dynamic weighting to apply the observer's reputation to the observation as part of the associative nature of the trust evaluation. If Yvette (user Y) observed Xavier (user X) and reported his behavior to Alice (user A), the system worked as follows. The performance observation ($obs_y(x)$) was weighted using the observing node's reputation ($RI_A(Y)$) before being integrated into the reputation calculation as feedback, shown in Equation 1. As explained above, $RI_A(Y)$ was the recipient's (in this case, Alice's) current RI value for the observer (who was Yvette.) The reporting node's current reputation was applied to the observation each time the FI was used. This method allowed the reputation-scaling method to consider the changes in observers' reputation values during the calculation of the RI .

$$FI = RI_A(Y) * obs_y(x) \quad \textbf{(1)}$$

Once the reports and observations had been gathered, they were merged and processed to provide a meaningful value that a node could use in making its trustworthiness evaluation. The reputation value needed to give a lagging or conservative approximation of the feedback input; trust with a healthy dose of skepticism, as it were. The system wanted to emphasize current behavior while, as discussed in previous sections, aging older input to diminish its impact on the reputation calculation. As in CORE[7] and CONFIDANT[8], a node maintained a reputation value for each peer that it associated with. Nodes entered the network with a reputation value of 0, giving new nodes a neutral level of trust. Similar to other reputation mechanisms, the expectation was that a node would naturally desire to have a positive reputation and any node with a negative reputation would be isolated as nodes refused to interact with it.

Using the previous example, we can explain how Equation 2 worked. We begin by assuming that Alice calculated Yvette's current RI (e.g.,)to be 0.65 previously. When Yvette shared a positive behavior grade on Xavier, Alice modified the behavior grade by Yvette's reputation so that the value of the FI was actually 0.65 (i.e., FI = 0.65 * 1). Because every node started with RI = 0, it was imperative that the first introduction be performed by the KMS.

This research developed the concept of a three-window weighted average (3Win). Modeled after a method of removing transients using batches or subsamples, this method divided a node's history into three weighted performance windows that revealed tendencies in a node's behavior. These windows were named Reputation Indexing Windows (RIW_S) and were numbered one through three, with RIW_1 containing the newest FIs and RIW_3 holding the oldest FIs. FIs were "pushed" through the windows (i.e., from RIW_1 to RIW_2 to RIW_3) as new FIs arrived. When an FI was pushed out of RIW_3 it was discarded.

When a node began collecting FI, a simple, unweighted average was used until RIW1 was filled. Once RIW_2 was started, the FIs were averaged within each RIW and the weights specified in Equation 3a applied. The weights changed when RIW_3 was established so that the RSM used Equation 3b.

The reporting rate of the nodes established the window sizes. The window size was directly related to the frequency of routine performance observations. Longer intervals between reports or fewer network nodes resulted in smaller sample sizes and therefore smaller window sizes, but this was not found to result in appreciable differences in reputation values. Heuristically, it was determined that the sum of the three window sizes should be 16% of the time period's total anticipated number of observations to produce a curve that ap-

FULL PAPER

proximated a node's behavior trend. The total window size was divided into a 10:30:60 ratio among the three windows (e.g., RIW_1:RIW_2: RIW_3). This ratio highlighted the most recent input (a small sample with the heaviest weight) and enabled a memory of past behavior with two larger but less weighted windows.

Nodes entered the network with a neutral reputation and started processing behavior feedback using Equation 2a, while RIW_1 and RIW_2 filled with FI. When the third window was established, the weights for each window shifted to those shown in Equation 2b. The second window was more heavily weighted than the third to emphasize the more recent input.

$$For 1 < |FI| \le (|RIW_1| + |RIW_2|), \lambda = 0.66; \mu = 0.33 \quad \textbf{(2a)}$$
$$RI = (\lambda * RIW_1) + (\mu * RIW_2)$$

$$For 1 < |FI| \ge (|RIW_1| + |RIW_2|), \lambda = 0.66; \mu = 0.22; \nu = 0.11 \quad \textbf{(2b)}$$
$$RI = (\lambda * RIW_1) + (\mu * RIW_2) + (\nu * RIW_3)$$

The evaluation of the 3Win began with a lambda value of 0.66, to stress the importance of the most current input. Experiments with the values of the weights of the three windows showed that a lambda value of 0.66 produced a curve that was responsive to the latest changes in input value trends. The RSM allowed a node to recover its reputation after having received negative input through continued positive performance. The rehabilitation process was the result of aging input items by shifting them through the windows. While the 3Win method enabled a node to overcome past mistakes, it yielded a skeptical approximation of the input. A hysteretic effect was desirable because it forced nodes to demonstrate sustained good behavior, rather than reward them too quickly and allow them to oscillate around the trust threshold. Furthermore, the widowed technique gave the advantage of being able to produce the non-reputable evidence (i.e., the FIs in the windows) upon which the reputation had been calculated. This meant that the system could implement both dynamic FI weighting and the introduction process in the trust management system.

Dynamic weighting was a powerful tool for the reputation-scaling algorithm as it had a significant impact on nodes that had been observed or associated with misbehaving nodes. Dynamic weighting relied on the existence of a system memory to store the identities and observations of its associates. This memory function and design are described in the following section.

REFERENCES

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

[2] 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)**.

[3] 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)**.

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

[5] A.Abdul-Rahman, S.Hades; Supporting trust in virtual communities. Proceedings of 33rd Annual Hawaii International Conference on System Sciences, 4-7 Jan 2000, 1-9 **(2000)**.

[6] J.Liu, V.Issarny; Enhanced Reputation Mechanism for Mobile Ad Hoc Networks. Proceedings of 2d International Conference of Trust Management (iTrust 2004), Oxford, UK, 29 March-1 April 2004, 48-62 **(2004)**.

[7] P.Michiardi, R.Molva; CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad-hoc Networks. Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, 107-121 **(2002a)**.

[8] S.Buchegger, J.Y.Le Boudec; Performance analysis of the CONFIDANT protocol. Proceedings of the 3rd ACM International Symposium on Mobile Ad-Hoc Networking and Computing, Lausanne, Switzerland, 226-236 **(2002b)**.