Study of Verification of the Reputation Scaling Module of Trust Management System

Yonghui CAO[1, 2]
1, School of Economics & Management, Henan Institute of Science and Technology, Xin Xiang, 453003 ,China
2, School of Management, Zhejiang University, Hang Zhou,310058 ,China

Abstract
The trust management system (TMS) developed through this research effectively implements a decentralized access and permission management scheme. The Reputation Scaling module (RSM) was the heart of the TMS. Our Reputation Scaling module applied different levels of trust to reports and observations. RSM advanced the current state of the art by introducing a reputation scaling mechanism that maintained a memory of past behavior grades and observers. The RSM used this historical knowledge to apply the observer's current RI to any behavior grade he might have made. In addition to dynamic FI weighting, the RSM's 3Win reputation scaling equation provided a more conservative approximation, allowing smaller fluctuations in the node's reputation than other equations currently in use. This testing concluded that this conservative approach benefited the network because it forced nodes to sustain positive behavior for longer periods than was necessary in the WMA or other reputation management mechanisms to achieve the same positive reputation. Each node gathered and processed feedback to calculate a usable RI for its peers. The TMS implemented an Trust model to represent the reputations that were compiled by a node on each of its peers.

Keywords:*Reputation Scaling, Inter-networking Mobility, Dynamic Collaborative Environment*

1 .Verification testing Goals and Objectives

Verification in engineering or quality management systems, it is the act of reviewing, inspecting or testing, in order to establish and document that a product, service or system meets regulatory or technical standards. Verification determined that each module had correctly transformed its inputs into the expected output. This testing involved isolating each function of each module by the arrangement of input and processing parameters. Specific outputs were then analyzed to check their correspondence to expected results. In general, verification testing revealed that the modules worked in accordance with the requirements. Verification theory is a theory relating the meaning of a statement to how it is verified.

Simulation models are increasingly being used in problem solving and to aid in decision-making. The developers and users of these models, the decision makers using information obtained from the results of these models, and the individuals affected by decisions based on such models are all rightly concerned with whether a model and its results are "correct". This concern is addressed through model validation and verification. Once basic verification was complete, performance boundary analysis was conducted to ascertain under which conditions the module operated best and under which conditions performance was impaired. Once these expectations were met, the modules were combined and the system validated. The following sub-sections provide the analysis of verification testing. These sub-sections follow a standard methodology (Bryce, Dimmock et al. 2005) is that： First，defining the role of each component. Second， analyzing the component to determine how module failure or impaired performance influences overall system functioning.

2. Reputation Scaling

The trust management system (TMS) developed through this research effectively implements a decentralized access and permission management scheme. Each resource owner uses the linked characteristics of identity, reputation, and risk to make access decisions. Because the TMS tracks a user’s behavior, using past behavior as future performance, no a priori user configuration is required. The TMS also offers a unique ability to enforce multiple access levels without the burden of implementing and managing multiple cryptographic keys or hierarchies of roles. A node provides its peers customized views of its contents and services based on its individual trust profile and the peer’s trustworthiness. As peers’ reputations change, their access changes to safeguard the node’s

resources for those peers that have shown themselves to contribute to the node's and the coalition's goals.
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 were no implied structural or system safeguards. 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 (RSM) was the heart of the TMS. The RSM's purpose was to implement a quantitative method for aggregating behavior feedback items (FIs) to generate a reputation value for each associate. A node used this value, called a Reputation Index (RI), as a measure of the trustworthiness he had of a specific network peer based on the peer's previous behavior. The RSM responded to the fluid nature of the Dynamic Collaborative Environment (DCE) by re-evaluating the source of each behavior grade before using the grade as input to the reputation scaling equation. The end result of this equation was a substantiated reputation index (RI) that was provided to the TMS. The RI was then compared against the trust thresholds to determine whether or not the system should extend trust and grant access to the requested resource.
If the RSM failed during operation, the TMS would have no way of processing behavior information or judging an associate's trustworthiness. The TMS would have to abandon a trust-based approach and resort to pre-configured access control methods, such as RBAC or identity-based mandatory access controls (MAC.) Neither method was considered acceptable in a DCE, for reasons discussed elsewhere in this research.

The RSM's approach had the following characteristics. It:

(1) Was node-centric, so that each node calculated only the reputations of the peers it was concerned with;
(2) Weighted FI to emphasize current behavior trends while accounting for past performance;
(3) Merged behavior reports (first-hand experiences) with observations (second-hand remarks);
(4) Aged FI over time to remove outdated behavior information;
(5) Enabled nodes to recover their reputation by demonstrating desirable behavior.

Verification of the RSM required the reputation scaling equation to produce a RI that conservatively estimates the observed peer's actual behavior. Next section compares the RSM's performance to the actual behavior grade and commonly used estimation techniques, such as the exponential weighted moving average.

3 .General Testing

We have developed a system where user nodes cooperated to exchange behavior reports and establish a record of each node's behavior history. This history, based on reports and observations, was expressed as a reputation index (RI). The RI, with evidence in the form of signed FIs, provided an expectation of their partner's behavior before entering into or dissolving an SA. By providing an indication of each other's trustworthiness, nodes avoided misbehaving nodes. The TMS that is installed on each node. In the following sections, this paper discusses how the TMS implements each of McKnight and Chervany's constructs to produce an access control decision. The RSM was tested to verify that the RI output by the module displayed a hysterisis effect with respect to its input, as shown in Figure 1. As the recording node (e.g., Joe) moved through different network conditions, the RSM was expected to produce results that accurately reflected the original input as the recording node (e.g., Joe) moved through different network conditions. In testing the RSM, the 3Win method was compared against the original input and the exponential weighted moving average equation used by Buchegger (Buchegger and Le Boudec 2002b). Comparing 3Win to the actual input and an exponential weighted moving average (WMA), Figure 1 shows how the RSM produced an RI that lagged behind the changes in behavior, as desired.

In the subsequent tests, we wanted to investigate the RMS's response in mobile situations. Interactivity traces were constructed using MATLAB and a Random Waypoint model. A 100 node network was constructed inside a 1000 x 1000 meter area. Each simulation was run for 1000 seconds. Humans developed a concept of reputation as an aggregation of trust information. They used this concept to predict the actions of others based on historical behavior information gained through personal interaction or the shared observations of peers. Researchers pointed out that reputation could be utilized in a virtual society, such as a MANET, to make up for the lack of the physical, interpersonal clues that humans use to determine trustworthiness.

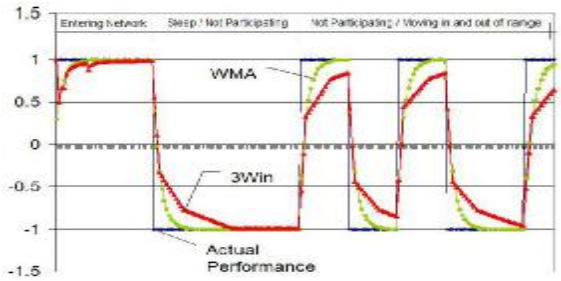

Fig. 1 the Hysterisis Effect of the 3Win Method

Scenarios were designed to test the ability of a RSM to:

- Identify selfish behavior,
- Allow a node to rehabilitate its reputation following a period of poor connectivity, and
- Respond to nodes that try to denigrate other nodes with undeserved negative performance observations.

In addition to these three performance measures, testing also needed to gauge the impact of dynamic FI weighting. Dynamic FI weighting linked and maintained the identity of the reporting node with the observation. The reporting node's current reputation (i.e., the RI value at the time of the calculation) was applied to the observation each time the RI was calculated. This method allowed the reputation scaling method to consider the changes in observers' reputation values during the calculation of the RI.

In each test, a node (e.g., Joe) received FI generated from observations and formal reports. The data set represented a period of approximately one hour of operation in the test bed and was distributed in the interval [-1,1] based on the previously described movement and behavior-based scenarios. Nodes provided observations on a 10-12 second interval. In all of the following graphs, the X-axis represents the passage of time and the Y-axis is the value of the node's RI.

The "unreliable node" scenario, shown in Figure 2, tested the RSM's flexibility in allowing a formerly unreliable node (e.g., Bob) to rehabilitate the reputation value that Joe maintained for him as Bob moved in and out of the Joe's transmission range. After a period of mobility, Bob relocated to a position with more stable connectivity and resumed cooperating with the network. Joe's associates observed and commented on Bob's behavior, providing the behavior grading that Joe fed to his RSM.

Because the periods of positive and negative observations were balanced, it was expected that the RSM would allow Bob to rebuild his reputation as he moved into the operating range of his peers. Figure 2 illustrates the performance of the two reputation scaling methods in the "unreliable node" scenario. Of note is the sharply fluctuating, optimistic curve that is produced by the WMA method. The 3Win mechanism produced an RI curve that was a smoother and more conservative approximation of the input while also allowing reputation rehabilitation.

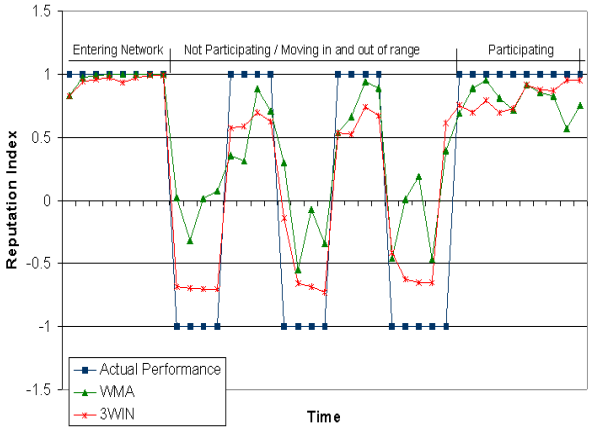

Fig. 2 Performance of Reputation-Scaling Mechanisms in an "Unreliable Node" Scenario

Points where the 3Win curve departed drastically from the WMA showed the effects of dynamically weighting observations. Because of its lack of history, the WMA method could only weight the most current observation and then only at the time it was applied to the reputation calculation. The 3Win method reapplied the weights of the observers at each calculation. As the observers' reputations changed, the value of their recommendations (in the form of FIs), changed as well.

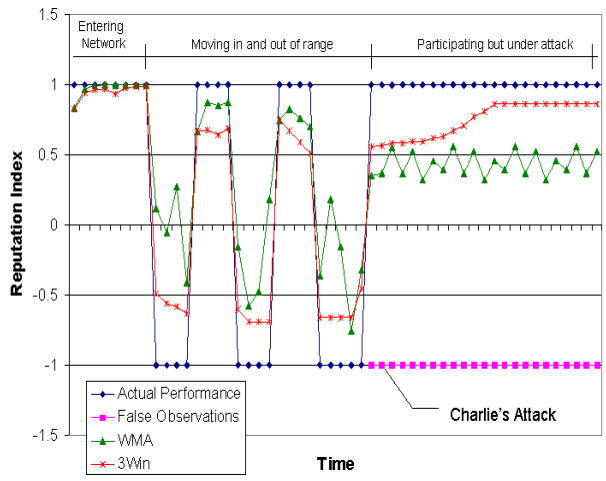

Fig. 3 Performance of Reputation-Scaling Mechanisms in a "Smear" Scenario

The "smear" scenario tested the efficiency of the reputation management mechanisms at resisting attacks on a node's reputation (see Figure 3). The observed node (again we'll use Bob) moved into the observer's (e.g., Joe's) operational area and should have been receiving positive feedback but Charlie tried to smear Bob's reputation by maliciously reporting negative feedback. The results show that the reputation management methods resisted the attack by dynamically weighting the FI, effectively diminishing Charlie's ability to impact Bob's reputation. When Charlie (the smearing node) was determined to be malicious, his reports were discounted and allowed Bob's reputation to recover.

The 3Win method provided a more conservative approximation, allowing smaller fluctuations in the node's reputation than the WMA. This testing concluded that this conservative approach benefited the network because it forced nodes to sustain positive behavior for longer periods than was necessary in the WMA or other reputation management mechanisms.

4 .Inter-networking Mobility Testing

Each node gathered and processed feedback to calculate a usable RI for its peers. The TMS implemented an Trust model 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 direct and not transitive. The following summarizes the trust model:

- Trust was context dependent.
- Trust had positive and negative degrees of trustworthiness.
- Trust was expressed in continuous values, as described by Marsh.
- Trust was based on experiences and observations between individuals.
- Trust information was exchanged between nodes.
- Trust was subjective. Nodes calculated different reputation values for the same observed node.
- Trust was dynamic and was modified, in a positive or negative direction, based on new observations and reports.

Once the reports and observations had been gathered, they were processed to provide a meaningful value that a node used for its trustworthiness evaluation. The reputation value needed to give a conservative approximation of the feedback input. We also wanted to emphasize current behavior while aging older input to diminish its impact on the reputation calculation. As in CORE and CONFIDANT, a node maintained a reputation value for each TP. Nodes entered the network with a reputation value of 0, a basic level of trust. Our expectation was that a node would desire a positive reputation. A node with a negative reputation would be isolated as nodes refused to interact with it.

Our Reputation Scaling module applied different levels of trust to reports and observations. Nodes placed full trust in KMS reports. On the other hand, periodic observations from other peers and friends were weighted using the reporting node's reputation (RIx) before into the reputation calculation. These weighted observations were called Feedback Items (FIs).

The test, displayed in Figure 4, showed the system acting on the test vignettes designed in Appendix A. The scenario began in the Tactical Operations Center (TOC), a medium density network environment made up of "good" users. Joe entered the network and associated himself with peers in the area, such as Alice. The presence of unreliable user behavior increased the trust thresholds but did not require any associations to be dissolved. When a "bad" user, Natasha, joined, she was not extended trust based on the information in the referrals received from Alice and other "good" users.

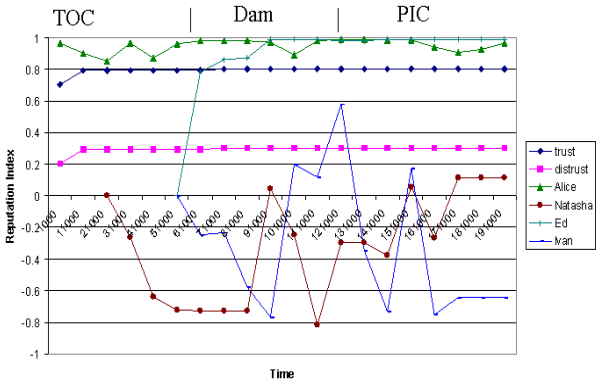

Fig. 4 Inter-Network Mobility Effects on Reputation Scaling

At time mark 61,000, Joe left the TOC and arrived at the Balcony Falls Dam to conduct a site survey. The Dam represented a sparse density, low population network environment of unreliable or resource-constrained users. Joe encountered Ed and, again based on referrals received from other associates, extended him trust while, at the same time, denying trust to Ivan, another "bad" user.

Finally, Joe entered the Public Information Center (PIC), a large, dense network of "bad" users. Having transitioned through two previous network environments, it was

important that Joe's RSM be able to continue to differentiate between desirable and undesirable associates. In other words, the RSM had to remember a sufficient amount of previous activity to re-establish or maintain association with people he met throughout the day. Although the presence of other "bad" users enabled Natasha and Ivan to improve their RIs slightly, their previous behavior still prevented them from gaining access to Joe's resources. At the same time, the "good" associates were maintained.

Figure 5 illustrates a situation where Joe's RSM was presented with a pair of "bad" users (Ivan and Natasha). This pair was actively colluding to subvert the network. The collusion was effected by having Ivan and Natasha only give each other positive observations while, at the same time, either not provide behavior grades or have them provide negative grades when none were warranted. In this manner, their plan was to allow Natasha to gain a foothold in the network by constructing associations with good users and then use these associations to insinuate Ivan, her confederate, into the network.

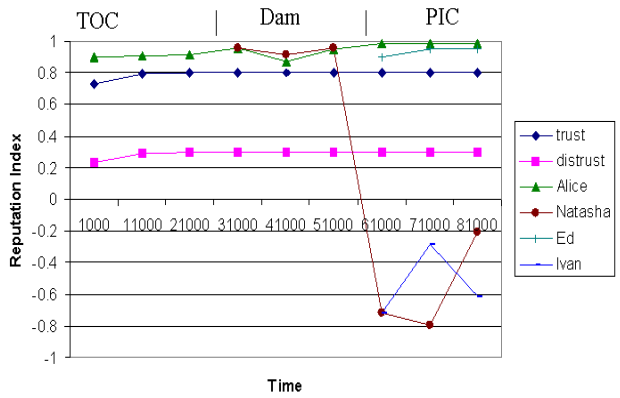

Fig. 5 Inter-Network Mobility with Collusion

Joe entered the network at the TOC, as in the previous test. He arrived at the Dam and was introduced to Natasha, who was performing as a good user. This association continued when Joe got to the PIC but he then observed that Natasha changed her behavior after she introduced her confederate, Ivan. Joe's RSM, recognizing that Natasha's behavior had become undesirable, lowered her RI as well as the RIs of those that she had introduced or referred. While at the PIC, Joe dissolved his association with Natasha but maintained her behavior history in his TS to enable him to weight her previous observations with her now unacceptably low RI. Furthermore, despite the collusion, Joe was still able to access Ed as a trustworthy sort and allowed him access.

These tests supported the validity of the RSM's performance. The RSM demonstrated the ability to maintain RIs on individual associates in varying network environments. Additionally, the use of dynamic weighting sped the process of identifying and isolating "bad" users by applying current reputations to RI calculation rather than depending on the observer's RI from the time of the observation.

Where Interpersonal trust was dependent upon peer behavior trends and System trust was determined through an evaluation of system behavior tendencies, Situational trust was independent of the behavior of other users altogether. This type of trust used the trust store, representing the user's memory of previous peers and situations, to determine what action it would take. A situational trust decision was predicated on remembering a previous decision that had yielded a positive outcome, regardless of the behavior of peers that may or may been involved.

5 .Contributions and Conclusion

Trust management offers the ability to make access control decisions in mobile ad-hoc collaborative environments without the need for pre-configuration or centralized management. By linking a node's identity to observations on its performance, its peers can calculate its reputation and evaluate its trustworthiness. Through a process of introduction, nodes share performance observations and are able to calculate reputations of newly encountered nodes in a peer to peer manner

The RSM advanced the current state of the art by introducing a reputation scaling mechanism that maintained a memory of past behavior grades and observers. The RSM used this historical knowledge to apply the observer's current RI to any behavior grade he might have made. This reevaluation was called dynamic FI weighting and it proved very successful in isolating not only misbehaving nodes but also nodes that might be colluding with them. In addition to dynamic FI weighting, the RSM's 3Win reputation scaling equation provided a more conservative approximation, allowing smaller fluctuations in the node's reputation than other equations currently in use. The RSM performed as expected and provided the TMS with a basis for trust decisions. It maintained correct reputation assessments on associates regardless of the characteristics of the other network users.

References

[1] Laird, J. and R. Wray (2011). Variability in Human Behavior Modeling for Military Simulations. Proceedings of the 2003 Conference on Behavior Representation in Modeling and Simulation (BRIMS), Scottsdale, AZ, Pp. 1-10.

[2] Krishnan, R., M. Smith, et al. (2011). "Economics of Peer-to-Peer Networks." Journal of Information Technology Theory and Application 5(3): 31-44

[3] Keser, C (2010). "Experimental games for the design of reputation management systems." IBM Systems Journal 42(3): 498-506.

[4] Commander Taco. (2010).”Slashdot." Retrieved 15 December, 2005, from http://slashdot.or

[5] KuroShin. (2010). "KuroShin." Retrieved 15 December, 2005, from http://www.kuro5hin.org.

[6] Powazek, D. (2010). "Gaming the system: How moderation tools can backfire." Retrieved 15 December, 2005, from http://designforcommunity.com/essay8.html.

[7] Ben Salem, N., J.-P. Hubaux et al. (2009). Reputation-based Wi-Fi deployment protocols and security analysis. Proceedings of the 2nd ACM International Workshop on Wireless Mobile Applications, Philadelphia, PA, Pp. 29-40.

[8] Bryce, C., N. Dimmock, et al. (2009). Towards an Evaluation Methodology for Computational Trust Systems. Proceedings of the Third International Conference in Trust Management (iTrust 2005), Paris, FR, Pp. 289-304.

[9] Lo Presti, S., M. Butler, et al. (2009). A Trust Analysis Methodology for Pervasive Computing

Systems. Trusting Agents for trusting Electronic Societies. R. Falcone, S. Barber, J. Sabater and M. Singly Springer.

[10]A. Datta, S. Quarteroni, and K. Aberer, "Autonomous Gossiping: A self-organizing epidemic algorithm for selective information dissemination in mobile ad-hoc networks.," Ecole Polytechnique Federale de Lausanne 2010.

[11] W. J. Adams, G. C. Hadjichristofi, and N. J.Davis, "Calculating a Node's Reputation in a Mobile Ad-Hoc Network," presented at the 24th IEEE International Performance Computing and Communications Conference (IPCCC 2005),Phoenix, AZ, 2005.

[12] R. Jain, The Art of Computer Systems Performance Analysis. New York, NY: John Wiley & Sons, 2005.

[13] E. Gray, J.-M. Seigneur, Y. Chen, and C. Jensen,"Trust propagation in small worlds," presented at the First International Conference on Trust Management (iTrust2003), 2003.

[14] S. Buchegger and J.-Y. Le Boudec, "A Robust Reputation System for Mobile Ad-Hoc Networks," EPFL 2003.

[15] M. Prietula and K. Carley, "Boundedly rational and emotional agents - cooperation trust and rumor," in Trust and Deception in Virtual Societies, C. Castelfranchi and Y.-H. Tan, Eds. Norwood, MA: Kluwer Academic Publisher,2001, pp. 169 - 193.

[16] A. Fernandes, E. Kotsovinos, S. Ostring, and B. Dragovic, "Pinocchio: Incentives for honest participation In Global-Scale Distributed trust management," University of Cambridge, Cambridge, UK 2001.

[17] W. Adams, R. Thomas, and N. Davis, "Sizing the Credential Cache in a Trust-based Access Control System," submitted to IEEE Global Telecommunications Conference (GLOBECOM 2005), St. Louis, MO, 2001.

Author Yonghui Cao received the MS degree in business management from Zheji**ang** University in 2006. He is currently a doctorate candidate in Zhejiang University. His research interest is in the areas of management information systems.