Volume No:1, Issue No:7 (December-2015) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

Active User A Computational Power of Belief Model

K.Mamatha

Assistant Professor,

Department of Computer Science and Engineering,

Christu Jyothi Institute of Technology and Science.

ABSTRACT:

Development of authorization mechanisms for secure information access by a large community of users in an open environment is an important problem in the ever-growing Internet world. In this paper we propose a computational dynamic trust model for user authorization, rooted in findings from social science. Unlike most existing computational trust models, this model distinguishes trusting belief in integrity from that in competence in different contexts and accounts for subjectivity in the evaluation of a particular trustee by different trusters. Simulation studies were conducted to compare the performance of the proposed integrity belief model with other trust models from the literature for different user behavior patterns. Experiments show that the proposed model achieves higher performance than other models especially in predicting the behavior of unstable users.

I.INTRODUCTION:

Many existing reputation models and security mechanisms rely on a social network structure. Pujol et al. propose an approach to extract reputation from the social network topology that encodes reputation information. Walter et al. propose a dynamic trust model for social networks, based on the concept of feedback centrality. The model, which enables computing trust between two disconnected nodes in the network through their neighbor nodes, is suitable for application to recommender systems. Lang proposes a trust model for access control in P2P networks, based on the assumption of transitivity of trust in social networks, where a simple mathematical model based on fuzzy set membership is used to calculate the trustworthiness of each node in a trust graph symbolizing interactions between network nodes. The mainstream research efforts for user authorization mechanisms in environments where a potential user's permission set is not predefined, mostly focus on role-based access control (RBAC), which divides the authorization process into the role-permission and user role assignment.

The existing approaches do not consider "context" as a factor affecting the value of trust, which prevents an accurate representation for real life situations. In this work, we propose a computational dynamic trust model for user authorization. Mechanisms for building trusting belief using the first-hand (direct experience) as well as second-hand information (recommendation and reputation) are integrated into the model. The contributions of the model to computational trust literature are: The model is rooted in findings from social science, i.e., it provides automated trust management that mimics trusting behaviors in the society, bringing trust computation for the digital world closer to the evaluation of trust in the real world. Unlike other trust models in the literature, the proposed model accounts for different types of trust. Specifically, it distinguishes trusting belief in integrity from that in competence. The model takes into account the subjectivity of trust ratings by different entities, and introduces a mechanism to eliminate the impact of subjectivity in reputation aggregation.Distinguishing between integrity and competence allows the model to make more informed and fine-grained authorization decisions in different contexts. The trust model we propose in this paper distinguishes integrity trust from competence trust.

II. RELATED WORK

2.1 MCKNIGHT'S TRUST MODEL:

The social trust model, which guides the design of the computational model in this paper, was proposed by McKnight and Chervany [16] after surveying more than 60 papers across a wide range of disciplines. It has been validated via empirical study [15]. This model defines five conceptual trust types: trusting behavior, trusting intention, trusting belief, institution-based trust, and disposition to trust. Trusting behavior is an action that increases a truster's risk or makes the truster vulnerable to the trustee. Trusting intention indicates that a truster is willing to engage in trusting behaviors with the trustee. A trusting intention implies a trust decision and leads to a trusting behavior. Two subtypes of trusting intention are:

Volume No:1, Issue No:7 (December-2015)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

1) Willingness to depend: the volitional preparedness to make oneself vulnerable to the trustee.
2) Subjective probability of depending: the likelihood that a truster will depend on a trustee.
Trusting belief is a truster's subjective belief in the fact that a trustee has attributes beneficial to the truster. The following are the four attributes used most often:
1) Competence: a trustee h-as the ability or expertise to perform certain tasks.
2) Benevolence: a trustee cares about a truster's interests.
3) Integrity: a trustee is honest and keeps commitments.
4) Predictability: a trustee's actions are sufficiently consistent.
Institution-based trust is the belief that proper structural conditions are in place to enhance the probability of achieving a successful outcome. Two subtypes of institution-based trust are:
1) Structural assurance: the belief that structures deployed promote positive outcomes. Structures
include guarantees, regulations, promises etc.
2) Situational normality: the belief that the properly ordered environments facilitate success outcomes. Disposition to trust characterizes a truster's general propensity to depend on others across a broad spectrum of situations. Two subtypes of disposition to trust are:
1) Faith in human: The assumptions about a general trustee's integrity, competence, and benevolence.
2) Trusting stance: A truster's strategy to depend on trustees despite his trusting belief about them. Trust intention and trusting belief are situation and trustee specific. Institution-based trust is situation specific. Disposition to trust is independent of situation and trustee. Trusting belief positively relates to trusting intention, which in turn results in the trusting behavior. Institution-based trust positively affects trusting belief and trusting intention. Structural assurance is more related to trusting intention while situational normality affects both. Disposition to trust positively influences institution-based trust, trusting belief and trusting intention. Faith in humanity impacts trusting belief. Trusting stance influences trusting intention.

2.2 COMPUTATIONAL TRUST MODELS:

The problem of establishing and maintaining dynamic trust has attracted many research efforts. One of the first attempts trying to formalize trust in computer science was made by Marsh [13]. The model introduced the concepts widely used by other researchers such as context and situational trust. Many existing reputation models and security mechanisms rely on a social network structure [1]. Pujol et al. propose an approach to extract reputation from the social network topology that encodes reputation information [19]. Walter et al. [22] propose a dynamic trust model for social networks, based on the concept of feedback centrality. The model, which enables computing trust between two disconnected nodes in the network through their neighbor nodes, is suitable for application to recommender systems. Lang [9] proposes a trust model for access control in P2P networks, based on the assumption of transitivity of trust in social networks, where a simple mathematical model based on fuzzy set membership is used to calculate the trustworthiness of each node in a trust graph symbolizing interactions between network nodes. Similarly, Long and Joshi [11] propose a Bayesian reputation calculation model for nodes in a P2P network, based on the history of interactions between nodes. Wang and Wang [23] propose a simple trust model for P2P networks, which combines the local trust from a node's experience with the recommendation of other nodes to calculate global trust. The model does not take the time of feedback into consideration, which causes the model to fail in the case of nodes with changing behavior. Reliance on a social network structure limits wide applicability of the mentioned approaches, especially for user authorization. FCTrust [8] uses transaction density and similarity to calculate a measure of credibility of each recommender in a P2P network. Its main disadvantages are that it has to retrieve all transactions within a certain time period to calculate trust, which imposes a big performance penalty, and that it does not distinguish between recent and old transactions. SFTrust [25] is a double trust metric model for unstructured P2P networks, separating service trust from feedback trust. Its use of a static weight for combining local and recommendation trust fails to capture node specific behavior.

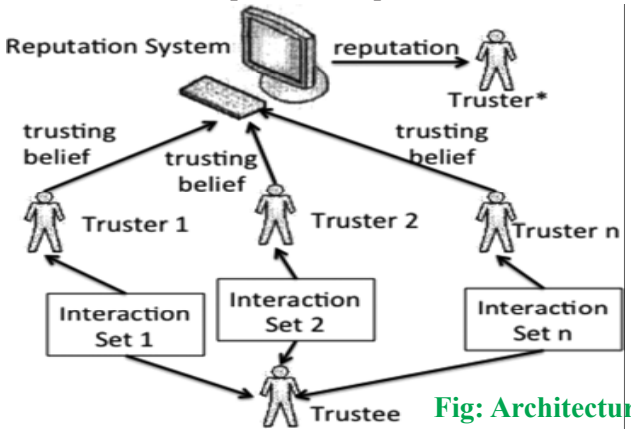

Fig: Architecture

Volume No:1, Issue No:7 (December-2015) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

Competence Belief Belief about a trustee's competence is context specific. A trustee's competence changes relatively slowly with time. Therefore, competence ratings assigned to her are viewed as samples drawn from a distribution with a steady mean and variance. Competence belief formation is formulated as a parameter estimation problem. Statistic methods are applied on the rating sequence to estimate the steady mean and variance, which are used as the belief value about the trustee's competence and the associated predictability. Estimation of Dmi and ci

III.BASED ON PREVIOUS KNOWLEDGE:

Two trusters become acquainted if they share a set of commonly rated trustees. It is assumed that a truster uses the consistent rating criteria for all trustees. Dmi and ci are estimated by comparing the trusting beliefs about trustees known by both t_ and ti. DmI and ci are computed using (15a) and (15b). This approach is named as competence reputation evaluation based on knowledge (CRE-K). The prerequisite of CRE-K is that the reputation requester has a set of commonly rated trustees with each of the trusters who provide the trusting beliefs. Suppose t_ is the truster who requests information. We want to evaluate Dmi for truster ti. Let fu1; u2; . . . ; ung be the trustees about whom both t_ and ti submit trusting beliefs, denote the competence trusting beliefs from t_ and ti respectively.Estimation Based on Priori Assumptions The second method to estimate Dmi and ci is based on priori assumptions about the distribution of trusters. This method uses the second estimator of s2_ , i.e., (17b). Instead of estimating each Dmi and ci, this method estimates based on assumptions and uses them to substitute ð Pk i¼1 DmiÞ=k and ci in (16) and (17b).This approach is named as competence reputation evaluation based on assumption (CRE-A). Study on Integrity Belief Building Methods In this section, the BDES algorithm is compared with three other algorithms for five trustee behavior patterns. Algorithms compared. The algorithms compared are BDES, simple average, single exponential smoothing, and the time-weighted average, called REGRET, proposed in [20]. Let ti denote the trusting belief after observing rating sequence r1; r2; . . . ; ri. Table 6 summarizes how ti is evaluated under the four algorithms. w(k, i) in REGRET is a time dependent function giving higher values to ratings temporally close to ri. Table 7 shows the initial values of the parameters of BDES and SES. A function linearly decreasing with (i – k) is used as w(k, i) in REGRET.

IV. CONCLUSION:

In this paper we presented a dynamic computational trust model for user authorization. This model is rooted in findings from social science, and is not limited to trusting belief as most computational methods are. We presented a representation of context and functions that relate different contexts, enabling building of trusting belief using crosscontext information. The proposed dynamic trust model enables automated trust management that mimics trusting behaviors in society, such as selecting a corporate partner, forming a coalition, or choosing negotiation protocols or strategies in e-commerce. The formalization of trust helps in designing algorithms to choose reliable resources in peer-to-peer systems, developing secure protocols for ad hoc networks and detecting deceptive agents in a virtual community. Experiments in a simulated trust environment show that the proposed integrity trust model performs better than other major trust models in predicting the behavior of users whose actions change based on certain patterns over time.

REFERENCES:

[1] G.R. Barnes and P.B. Cerrito, "A Mathematical Model for Interpersonal Relationships in Social Networks," Social Networks, vol. 20, no. 2, pp. 179-196, 1998.

[2] R. Brent, Algorithms for Minimization without Derivatives. Prentice- Hall, 1973.

[3] A. Das and M.M. Islam, "SecuredTrust: A Dynamic Trust Computation Model for Secured Communication in Multiagent Systems," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 2, pp. 261-274, Mar./Apr. 2012.

[4] C. Dellarocas, "Immunizing Online Reputation Reporting Systems against Unfair Ratings and Discriminatory Behavior," Proc. Second ACM Conf. Electronic Commerce, pp. 150-157, 2000.

[5] L. Fan, "A Grid Authorization Mechanism with Dynamic Role Based on Trust Model," J. Computational Information Systems, vol. 8, no. 12, pp. 5077-5084, 2012.

[6] T. Grandison and M. Sloman, "A Survey of Trust in Internet Applications," IEEE Comm. Surveys, vol. 3, no. 4, pp. 2-16, Fourth Quarter 2000.

Volume No:1, Issue No:7 (December-2015)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

[7] J.D.Hamilton, TimeSeriesAnalysis. PrincetonUniversity Press, 1994.

[8] J. Hu, Q. Wu, and B. Zhou, "FCTrust: A Robust and Efficient Feedback Credibility-Based Distributed P2P Trust Model," Proc. IEEE Ninth Int'l Conf. Young Computer Scientists (ICYCS '08), pp. 1963-1968, 2008.

[9] B. Lang, "A Computational Trust Model for Access Control in P2P," Science China Information Sciences, vol. 53, no. 5, pp. 896-910, May 2010.

[10] C. Liu and L. Liu, "A Trust Evaluation Model for Dynamic Authorization," Proc. Int'l Conf. Computational Intelligence and Software Eng. (CiSE), pp. 1-4, 2010.

[11] X. Long and J. Joshi, "BaRMS: A Bayesian Reputation Management Approach for P2P Systems," J. Information & Knowledge Management, vol. 10, no. 3, pp. 341-349, 2011.

[12] S. Ma and J. He, "A Multi-Dimension Dynamic Trust Evaluation Model Based on GA," Proc. Second Int'l Workshop Intelligent Systems and Applications, pp. 1-4, 2010.

[13] S. Marsh, "Formalizing Trust as a Concept," PhD dissertation- Dept. of Computer Science and Math., Univ. of Stirling, 1994.

[14] P. Matt, M. Morge, and F. Toni, "Combining Statistics and Arguments to Compute Trust," Proc. Ninth Int'l Conf. Autonomous Agents and Multiagent Systems (AAMAS '10), pp. 209-216, 2010.

[15] D. McKnight, V. Choudhury, and C. Kacmar, "Developing and Validating Trust Measures for E-Commerce: An Integrative Topology," Information Systems Research, vol. 13, no. 3, pp. 334-359, Sept. 2002.

[16] D. McKnight and N.L. Chervany, "Conceptualizing Trust: A Typology and E-Commerce Customer Relationship Model," Proc. 34th Ann. Hawaii Int'l Conf. System Sciences (HICSS '01), 2001.

[17] W. Mendenhall and R.J. Beaver, Introduction to Probability and Statistics. PWS-Kent Publishing Company, 1991.

[18] A. Nagarajan and V. Varadharajan, "Dynamic Trust Enhanced Security Model for Trusted Platform Based Services," Future Generation Computer Systems, vol. 27, pp. 564-573, 2011.

[19] J.M. Pujol, R. Sangesa, and J. Delgado, "Extracting Reputation in Multi Agent Systems by Means of Social Network Topology," Proc. Int'l Conf. Autonomous Agents and Multiagent Systems (AAMAS '02), pp. 467-474, 2002.

[20] J. Sabater and C. Sierra, "Social ReGreT, a Reputation Model Based on Social Relations," ACM SIGecom Exchanges, vol. 3, no. 1, pp. 44-56, 2002.