A DIGITAL SIGNATURES –BASED TRUST SECURED MANAGEMENT SYSTEM FOR MULTI-AGENT NETWORKS

Parkavi. D
II M.E, Computer Science and Engineering,
Maharaja Engineering College for Women, Perundurai, India

Abstract

In Multi- Agent System, malicious agents are always seeking ways of exploiting any existing weakness in the network. Existing system analyzes the different factors related to evaluating the trust of an agent and then proposes a comprehensive quantitative model for measuring such trust. A novel load-balancing algorithm based on the different factors defined is proposed. Simulation results indicate that our model compared to other existing models can effectively cope with strategic behavioral change of malicious agents and at the same time efficiently distribute workload among the service providing agents under stable condition. In existing system key generation is handling by static key process. In proposed system, a Digital signature is used to employ a type of asymmetric cryptography. A properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender.

Index Terms— Multi-Agent Systems (MASs), EigenTrust, SecuredTrust, Feedback credibility, reputation, load balancing, malicious behavior.

1. Introduction

Multi-Agent Systems (MAS) are increasingly becoming popular in carrying valuable and secured data over the network. The open and dynamic nature of MAS has made it a challenge for researchers to operate MAS in a secured environment for information transaction. In a multi-agent system, agents interact with each other to achieve a definite goal that they cannot achieve alone and such systems include P2P , grid computing, the semantic web, pervasive computing and MANETs. Since malicious agents are always seeking ways of exploiting any existing weakness, trust and reputation play a critical role in ensuring effective interactions among the participating agents [3]. Trust issues have become more and more popular since traditional network security cannot predict agent behavior from a 'trust' viewpoint.

2. Related Work

2.1 Web Features

In the field of E-Commerce, a compelling list of Web attributes that engender trustworthiness is generated. For example, one commonly cited study has identified six features of Web sites that enhance the marketer's trustworthiness. These Web features include: (1) safeguard assurances, (2) the marketers' reputation, (3) ease of navigation, (4) robust order fulfillment, (5) the professionalism of the Website, and (6) the use of state-of-the-art Web page design technology.

2.2 Scope of Trust

Most of the studies examining the impact of Web features on consumer trust and purchasing behavior rely on two primary kinds of evidence: consumers' retrospective reports and views of experts. Relying on consumer retrospective reports may introduce confounds such as purchasing histories and the nature of the established relationship with the marketer. Purchasing histories will introduce biases of product or brand preferences, while the use of current customers ignores the impact of the nature (impersonal or personalized) and stage (i.e. attraction, maintenance, etc.) of the trust building relationship. The present study uses an experimental design to investigate trust in business to consumer (B2C) e-commerce**.**

1. What is the role of four commonly used Web privacy and security attributes in evoking consumer willingness to purchase online?
2. What role does trustworthiness play in a consumer's interaction with Web merchants?
3. What role does web design have in the consumer purchase decision?

Before addressing these questions, this paper clarifies a few definitional ambiguities and briefly reviews the relevant literature. Particular attention is given to B2C e-commerce.

2.3 Trust Management Approaches

There exist currently two different major approaches for managing trust: policy-based and reputation-based trust management. These approaches have been developed within the context of different environments and targeting different requirements. The policy-based trust relies on objective "strong security" mechanisms such as signed certificates and trusted certification authorities (CA) in order to regulate the access of users to services. The access decision is usually based on mechanisms with well defined semantics (e.g., logic programming) providing strong verification and analysis support. The policy-based trust management approach usually results in binary decision according to which the requester is trusted or not, and thus the service is allowed or denied. Reputation-based trust relies on a "soft computational" approach to the problem of trust [8] [9]. In this case, trust is typically computed from local experiences together with the feedback given by other entities in the network (e.g., users who have used services of that provider). For instance, in eBay buyers and sellers rate each other after each transaction. The ratings pertaining to a certain seller (or buyer) are aggregated by the eBay's reputation system into a number reflecting seller (or buyer) trustworthiness as seen by the eBay community. The reputation-based approach has been favored Peer-to-Peer or Semantic Web, where certifying authorities could not be always assumed but where a large pool of individual user ratings was usually available.

3. A Robust and Scalable Reputation System

Building an efficient P2P reputation system is a challenging task. The six key issues that should be addressed in the design of an effective P2P reputation system are:

High accuracy: It helps to distinguish reputable peers from malicious ones. The system should calculate the reputation scores as close to the real trustworthiness as possible.

Fast convergence speed: The reputation in peer varies over time and the reputation aggregation should converge fast enough to reflect the true changes of peer behaviors.

Low overhead: The P2P system should consume limited computation and bandwidth resources for peer reputation evaluation [9].

Adaptive to peer dynamics: The system should adapt to the peer dynamics instead of relying on pre-determined peers.

Robust to malicious peers: The P2P system should be robust to the attacks by both independent and malicious peers.

Scalability: The P2P system should be able to serve a large number of peers in term of accuracy, convergence speed, and extra overhead per peer.

4. A Reputation-based Trust Model

Peer-to-peer (P2P) E-Commerce communities are often established dynamically with peers that are unrelated and unknown to each other. Peers of such communities have to manage the risk involved with the transactions without prior experience and knowledge about each other. Reputation systems provide a way for building trust through social control without trusted third parties [10]. Most research on reputation-based trust utilizes community-based feedback that is often a simple aggregation of positive and negative feedback and cannot accurately capture the trustworthiness of peers. In addition, peers can misbehave in a number of ways, such as providing false feedback on other peers. The challenge of building a reputation based trust mechanism is how to effectively cope with such malicious behavior of peers [11]. Another challenge is that trust context varies from community to community and from transaction to transaction. It is important for the trust model to be able to adapt to different communities and different situations. Furthermore, there is also a need for experimental evaluation methods of a given trust model in terms of effectiveness and benefits.

4.1 Trust Parameters

In PeerTrust, a peer's trustworthiness is defined by an evaluation of the peer in terms of its reputation in providing services to other peers in the past [2]. Such reputation reflects the degree of trust that other peers in the community have on the given peer based on their past experiences.Five important factors for evaluation are:The feedback about the amount of satisfaction a peer obtains through transactions with other peers.

1. The number of transactions the peer has performed with other peers, a scope factor for comparing the feedback among different peers
2. The credibility of peers who submit feedback, addressing the risk of using potentially false feedback to rate peers' reputation
3. The transaction context factor, addressing the impact of transaction characteristics (such as transaction size or type) on the trustworthiness of the peers [10].
4. The community context factor, addressing the impact of community-specific properties on the trustworthiness of peers.

4.2 The Basic Metric

The basic metric computes the trust value of a peer u using the three basic parameters by an average of the credible amount of satisfaction peer u receives for each transaction performed during a given period. Both the feedback and the number of transactions are quantitative measures and can be collected automatically. The third trust parameter credibility of feedback is a qualitative measure and needs to be computed based on past behavior of peers who gives feedback. The credibility factor is determined and the credible amount of satisfaction is computed. For example, one may use a function of the trust value of a peer as its credibility factor so feedback from trustworthy peers are considered more credible and thus weighted more than those from untrustworthy peers [3]. We believe that the study of what determines the precision of credibility of feedback is by itself an interesting and hard research problem that deserves attention of its own [4].

4.3 Adapting the Metric with Context Factor

The metric may take into account transaction context factor to capture the transaction-dependent characteristics. For example, if a community is business savvy, the size of a transaction is an important context that should be incorporated in the trust metric to weight the feedback for that transaction. It can act as a defense against some of the subtle malicious attacks, such as a seller develops a good reputation by being honest for small transactions and tries to make a profit by being dishonest for large transactions. Various community contexts can be taken into account to address some of the common problems. For example, the historical transaction history can be built into the metric through community context factor but with a lower weight than recent transaction history to add temporal adaptively. The problem of lack of incentives to rate or the free riding problem in file sharing communities can be also addressed by building incentives/awards for rating others or sharing files through community context factor. If a trust authority or pre-trusted peers are available in a community [12], their evaluation can be also built into the metric as community context factor to make the metric more robust against manipulation of malicious peers.\

5. Problem description

Business-to-Business (B2B) E-Commerce is defined as transactions conducted electronically between organizations [5]. Similarly, Internet shopping decisions involve trust not simply between the service provider and the consumer, but also between the consumer and the peer system on which transactions are executed. Although many studies have identified the critical role of consumer trust in Internet shopping, a critical issue has hampered empirical investigations of the impact of consumer trust on on-line purchasing activities. The issue is centered on the lack of agreement about the definition of online consumer trust**.**

Two questions baesd on the roles of consumers:

1.What role does trustworthiness play in a consumer's interaction with Web merchants?

2. What role does web design have in the consumer purchase decision?

A study in which a previously validated measurement instrument is used to investigate the existence and importance of specific factors that are thought to predict the generation of consumer trust in service.

6. Drawbacks in Existing System

Most of the existing global reputation models can successfully isolate malicious agents when the agents behave in a predictable way [1]. However, these models suffer greatly when agents start to show dynamic personality, i.e., when they start to behave in a way that benefits them. These models also fail to adapt to the abrupt change in agents' behavior and as a result suffer when agents alter their activities strategically.

Typically, reputation-based trust is used in distributed networks where a system only has a limited view of the information in the whole network [11]. New trust relationships are inferred based on the available information (following the idea of exploiting world's information). The available information is based on the recommendations and the experiences of other users, and it is typically not signed by certification authorities but sometimes self-signed by the source of the statement itself. This supports trust estimation with a wide range and allows the propagation of trust (e.g., transitive propagation) along the network as well as weighting of values.

7. Proposed system

In e-business environment, Trust Management is an important factor that is necessary for all transactions [5]. The basic e-business requirements like non-reputation of both trustee and of trustier are found to be problem arising due to lack of trust information. We now derive our main result: an agent's discount factor is a direct measure of its trustworthiness given assumptions. A key motivation for work on trust is that the primary interaction mechanism is not incentive compatible. And so, the agents would act honestly. Our desiderata not only apply well. A desirable system must be:

EVIDENTIAL: An agent should use evidence-based trustworthiness measurements to predict the agent's future behavior in the system. Thus the trust system can act upon its knowledge. **AGGREGABLE:** Trustworthiness measurements should be accurate, precise, and possible to aggregate. Aggregation enables an agent to communicate about trustworthiness and the indirect information is obtained from other agents to increase knowledge of trustworthiness.

FLEXIBLE: Trustworthiness should be applicable across multiple situations. Trustworthiness measurements should be achieved in products, services, and even interaction mechanisms.

LOAD BALANCING: we propose an algorithm for balancing loads among the trusted agents. The trust of agents who respond to a transaction request is determined and then the agent with the highest trust value is selected. The agent with the highest trust value will have immense workload while other capable agents with slightly lower reputation will have considerably less workload.

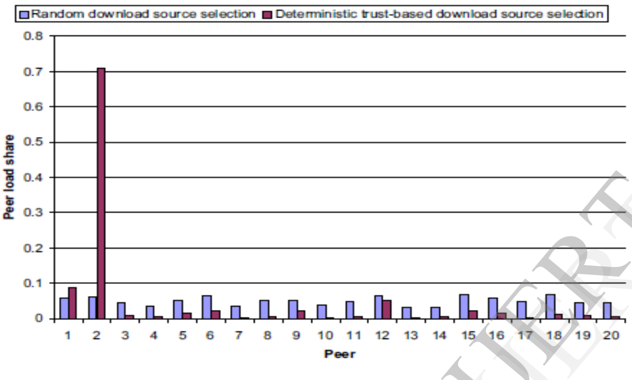

Figure 1 Load Balancing in Network

8. Conclusion

We have presented a novel trust computation model called SecuredTrust for evaluating agents in Multi-Agent environments. It can ensure secured communication among the agents by detecting strategic behaviors of malicious agents effectively[3]. In this paper, we have given a comprehensive mathematical definition of the different factors related to computing trust. A model for combining all these factors is provide to evaluate trust and finally, and a heuristic load-balancing algorithm for distributing workload among service providers is achieved. Compared to other existing trust models, Secured-Trust is more robust and effective against attacks from opportunistic malicious agents while capable of balancing load among service providers.

9. References

[1] N.R. Jennings, “An Agent-Based Approach for Building Complex Software Systems,” Comm. ACM, vol. 44, no. 4, pp. 35-41, 2001.

[2] R. Steinmetz and K. Wehrle, “Peer-to-Peer Systems and Applications”, Springer-Verlag, 2005.

[3] Anupam Das and M.Mahfuzul Islam,”SecuredTrust: A Dynamic Trust Computation Model for Secured Communication in Multi-Agent Systems”, IEEE,2012.

[4] Siddharth Maini “A Survey Study on Reputation-Based Trust Management in P2P Networks”,2005.

[5] L. Mui, M. Mohtashemi, and A. Halberstadt, “A Computational Model of Trust and Reputation for E-Businesses,” Proc. 35th Ann. Hawaii Int’l Conf. System Sciences (HICSS ’02), pp. 2431-2439, 2008.

[6] I.Foster, C. Kesselman, and S. Tuecke, “The Anatomy of the Grid: Enabling Scalable Virtual Organizations,” Int’l J. High Performance Computing Applications, vol. 15, no. 3, pp. 200-222, 2007.

[7] T. Berners-Lee, J. Hendler, and O. Lassila, “The Semantic Web,” Scientific Am., pp. 35-43, May 2010.

[8] M. Gupta, P. Judge, and M. Ammar, “A Reputation System for Peer-to-Peer Networks,” Proc. 13th Int’l Workshop Network and Operating Systems Support for Digital Audio and Video (NOSSDAV ’03), pp. 144-152, 2010.

[9] L. Mui, “Computational Models of Trust and Reputation: Agents, Evolutionary Games, and Social Networks,” PhD thesis, MIT, http://groups.csail.mit.edu/medg/medg/people/lmui/docs, Dec. 2010.

[10] Chris Burnett1, Timothy J. Norman1, and Katia Sycara, “Sources of Stereotypical Trust in Multi-Agent Systems”,2009.

[11] S.D. Ramchurn, D. Huynh, and N.R. Jennings, “Trust in Multi-Agent Systems,” The Knowledge Eng. Rev., vol. 19, no. 1, pp. 1-25,2009.

[12] P. Dasgupta, “Trust as a Commodity, Trust: Making and Breaking Cooperative Relations”, vol. 4, pp. 49-72, 2008.

[13] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman,“Reputation Systems,” Comm. ACM, vol. 43, no. 12, pp. 45-48, 2008.

[14] A.A. Selcuk, E. Uzun, and M.R. Pariente, “A Reputation-Based Trust Management System for P2P Networks,” Proc. IEEE Int’l Symp. Cluster Computing and the Grid (CCGRID ’04), pp. 251-258,2007.

[15] I.Foster, C. Kesselman, and S. Tuecke, “The Anatomy of the Grid: Enabling Scalable Virtual Organizations,” Int’l J. High Performance Computing Applications, vol. 15, no. 3, pp. 200-222, 2007.