ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

Improving Security in Multi-Agent Systems by Using a Novel Reputation Model

G.V.Pavan Kumar[1], J.Praveen Kumar[2]

Student, Department of CSE, MRCET, Hyderabad, India [1]

Assistant Professor, Department of CSE, MRCET, Hyderabad, India [2]

ABSTRACT--Multi-agent systems like Peer-to-Peer networks are widely used for content sharing and searching. However, privacy and security are the concerns with such networks as they are vulnerable to attacks due to open, dynamic and anonymous nature. To protect communications over such networks many models came into existence that are based on the reputation or trust of the peers that interact with each other. However, they can not cope with the unpredictable behavior of malicious peers. To overcome this problem and improve QoS (Quality of Service) Das and Islam presented a dynamic trust computation model. In this paper we implement that trust model and build a prototype of multi-agent system to show the proof of concept. The experimental results revealed that the application facilitates dynamic trust computation and achieves secure communication and quality of service by balancing load among the agents.

Index Terms – Peer-to-Peer networks, trust, trust management, malicious agents, load balancing

I. INTRODUCTION

Multi-agent systems like Gnutella are famous for their ease of use and utility in sharing and searching for content. They are examples for Wide Area Network (WAN). Multiple agents interact with each other to achieve the goal of the network. There are many such networks in the real world. They are part of grid computing [1], P2P (Peer to Peer) networks [2], [3], [4] and so on. The multi-agent systems like P2P are vulnerable to security attacks as they are anonymous, open and dynamic in nature. Some agents may get compromised and act like malicious agents. They spoil the secure communication over the network. In such scenarios where a multi-agent system is affected, computing the trust or reputation of such peers has become an important solution towards security in multi-agent systems [5], [6]. Trust and reputation theories have been around for long time. There are many existing trust models [7], [8], [9], [10] that protect multi-agent networks. These trust models let the nodes to determine the trust of other nodes and take decisions to avoid communication with malicious nodes as they to not have trust. There are two categories of reputation based trust models [11], [12]. They are known as local trust models and global trust models. Global trust models [13], [14], [15], [16], [17], [18], [19], [20], [21] take feedback from other agents who have already interacted with the target agent. Based on the feedback given by other nodes and the trust value of the target node, the source node makes decisions for sending information. There models are naturally complex. The local trust models on the other hand do not take feedback from other agents for making decisions while sending data or making a request. Many existing trust models work well when the malicious agents in multi-agent network behave predictably. However, when the nodes behave unpredictably, these models suffer from coping with them. They cannot handle attacks like collusion, unfair rating and dishonest rating. When peers misbehave it is difficult to estimate the load of peers as well. This is because the malicious peers show dishonest load and trust values. This is a challenging problem.

To overcome this problem Das and Islam [22] presented a dynamic trust computation model which considers various parameters to calculate trust. It achieves both security and server quality at a time. It does load balancing well. In this paper we implement this dynamic trust model by implementing a prototype multi-agent as proof of concept. The remainder of this paper is structured as follows. Section II reviews literature available. Section III presents experimental results while section IV concludes the paper.

II. RELATED WORK

Many existing trust models believed that the trust is multi-dimensional and the peers to evaluate trust from various perspectives. The existing trust models include Bayesian Network based trust model [14], EigenTrust [15]. The latter uses local trust computation to find out global trust value of an agent. It depends on pre-trusted nodes for recommendations. It has drawbacks such as lack of pre-trusted nodes and the compromised pre-trusted nodes. Similar to EigenTrust is the model proposed by Dou et al. [23] which does not depend on pre-trusted agents. It has mechanism to punish misbehaving agent but can't do anything with dishonest recommenders. This is its drawback. GeGreT [24], [25], [26] is another reputation model which considers three dimensions namely ontological, social and individual dimensions. Individual dimension reflects own observation of agent, social dimension refers to recommendations from other agents, and the ontological dimension is used to consider the trust as multi faceted concept. PeerTrust [16], [27] is another trust model which is computationally expensive and not viable. FCTrust [21] considers similarity measure and density for feedback whose main drawback is storage overhead. Two trust metrics are used by SFTrust [20] one for feedback trust and other for service trust. As its trust model is static over a period of time, it fails to estimate accurate trust values. FIRE [28], [29] is another trust model which considers trust from many sources including third party references, role based rules, witness information and direct experience. This model is suffers from susceptible behavior of nodes and dishonesty problems. Wang et al. [30] presented a recommendations model that combines local and global trusts. However, the trust of agents is static and it can't code with dynamic nature of the multi-agent network. Li et al. [19] proposed another trust model which makes use of expected trust, historical trust, and recent trust for trust computation. Due to historical trust values it causes storage overhead. Wen et al. [31] combines both indirect and direct trust computing with equal weights to all routes to target agent which is not a practical solution. The trust value of nodes should deteriorate over time which is not addressed in many models like [14], [15], [16], [17], [18], [19], [20]. To overcome this problem [30] and [32] introduced decay function. However, they fail to cope with real time dynamism.

Recently Das and Islam [22] proposed a dynamic trust model which uses decay function along with many other factors that were not considered by others. Besides dynamic trust computation, it also considers the problem of load balancing for satisfactory level of service quality.

III. EXPERIMENTAL RESULTS

We did experiments with the prototype application we built. The application runs in network with multiple agents. The trust computation algorithm runs in every node. As per the dynamic trust computation with various parameters, the communication takes place in the network with secure manner. The algorithm is also capable of dealing with malicious agents that show unpredictable behavior.

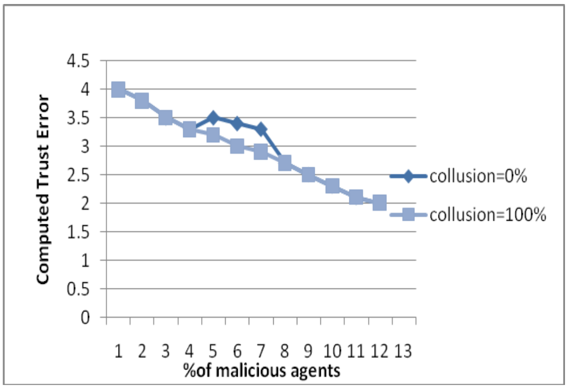

Fig. 1 - Trust computation error (RMS) with respect to percentage of malicious agents

As can be shown in figure 1 the horizontal axis represents the % of malicious agents while vertical axis represents the computed trust error.

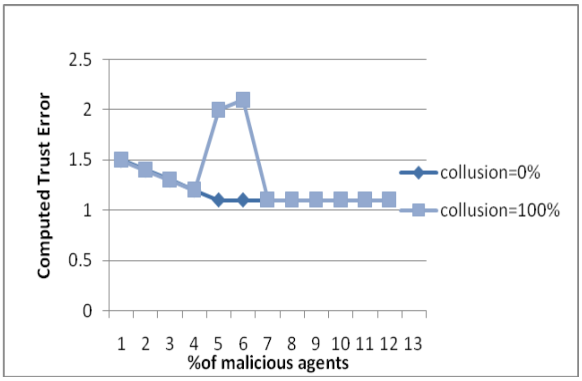

Fig. 2. Trust computation error (RMS) with respect to percentage of false response by malicious agents

As can be shown in above figure 2 the horizontal axis represents the % of malicious agents while vertical axis represents the computed trust error.

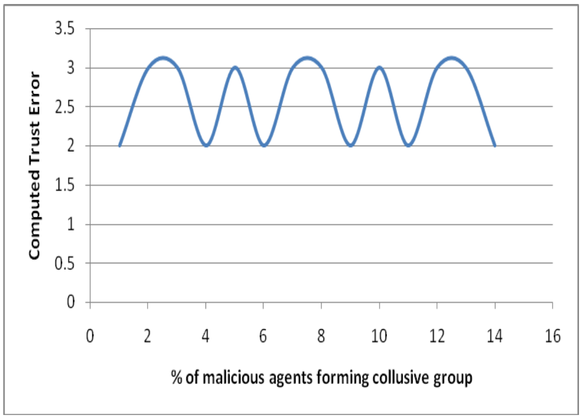

Fig. 3. Trust computation error with respect to percentage of malicious agents forming collusive group.

As can be shown in above figure 3 the horizontal axis represents the % of malicious agents forming collusive group while vertical axis represents the computed trust error.

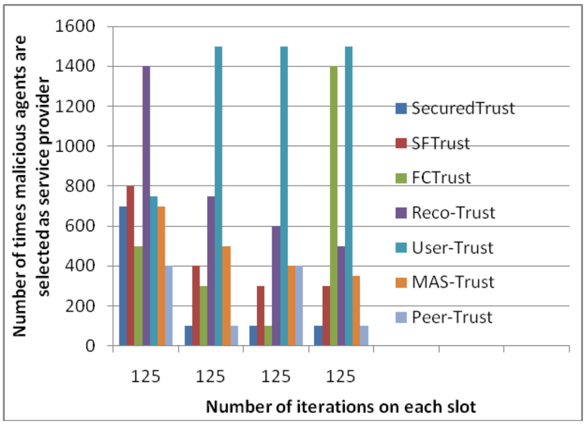

Fig. 4. Comparing Out work with other trust models in terms of the number of times malicious agents are selected as service providers. As can be shown in above figure 4 the horizontal axis represents the number of iterations on each slot while vertical axis represents number of times malicious agents are selected as service provider.

IV. CONCLUSON

The existing trust computation models fail to secure the communications over multi-agent networks when the nodes behave unpredictably. This is a challenging problem to be solved. Das and Islam proposed a dynamic trust computation model which can cope with malicious nodes and their unpredictable behavior. In this paper we have implemented the dynamic trust computation model where the trust is computed based on various factors including local trust, feedback taken from other agents, direct trust, and indirect trust and so on. By considering the trust computation dynamically the node which needs to communicate with other node can judge the trust of that node and make appropriate decisions. In the process, the proposed system also considers load balancing. When two nodes have trust with different load, then the application takes a decision to balance load of the nodes. We built a prototype multi-agent system which demonstrates the proof of concept. The experimental results are encouraging.

REFERENCES

[1] I. Foster, C. Kesselman, and S. Tuecke, “The anatomy of the grid: enabling scalable virtual organizations,” International Journal of High Performance Computing Applications, vol. 15, no. 3, pp. 200– 222, 2001.

[2] (2000) Gnutella. [Online]. Available: http://www.gnutella.com

[3] Kazaa. [Online]. Available: http://www.kazaa.com/

[4] (2000) edonkey2000. [Online]. Available: http://www.emule-project.net/

[5] S. D. Ramchurn, D. Huynh, and N. R. Jennings, “Trust in multi- agent systems,” The Knowledge Engineering Review, vol. 19, no. 1, pp. 1–25, 2004.

[6] P. Dasgupta, “Trust as a commodity,” Trust: Making and Breaking
Cooperative Relations, pp. 49–72, 2000.

[7] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, “Repu- tation systems,” Communications of the ACM, vol. 43, no. 12, pp. 45–48, 2000.

[8] A. A. Selcuk, E. Uzun, and M. R. Pariente, “A reputation-based trust management system for P2P networks,” in Proceedings of the 2004 IEEE International Symposium on Cluster Computing and the Grid (CCGRID), 2004, pp. 251–258.

[9] M. Gupta, P. Judge, and M. Ammar, “A reputation system for peer- to-peer networks,” in Proceedings of the 13th international workshop on Network and operating systems support for digital audio and video (NOSSDAV). ACM, 2003, pp. 144–152.

[10] K. Aberer and Z. Despotovic, “Managing trust in a peer-2-peer infor- mation system,” in Proceedings of the tenth international conference on Information and knowledge management (CIKM). ACM, 2001, pp. 310–317.

[11] L. Mui, M. Mohtashemi, and A. Halberstadt, “A computational model of trust and reputation for e-businesses,” in Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS’02), 2002, pp. 2431 – 2439.

[12] L. Mui, “Computational models of trust and

reputation: agents, evolutionary games, and social networks," Ph.D. Thesis, Massachusetts Institute of Technology(MIT), 2002. [Online]. Available: http://groups.csail.mit.edu/medg/medg/people/lmui/docs/

[13] F. Cornelli, E. Damiani, S. D. Capitani, S. Paraboschi, and P. Sama- rati, "Choosing reputable servents in a P2P network," in Proceedings of the 11th ACM World Wide Web Conference (WWW), May 2002, pp. 376–386.

[14] Y. Wang and J. Vassileva, "Bayesian network-based trust model," in Proceedings of IEEE/WIC International Conference on Web Intelligence (WI), Halifax, Canada, October 2003, pp. 372–378.

[15] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The EigenTrust algorithm for reputation management in P2P networks," in Proceedings of the 12th ACM international World Wide Web conference (WWW), 2003, pp. 640–651.

[16] L. Xiong and L. Li, "Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities," IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 7, pp. 843–857, 2004.

[17] M. Srivatsa, L. Xiong, and L. Liu, "TrustGuard: Countering vul- nerabilities in reputation management for decentralized overlay networks," in Proceedings of the 14th ACM international conference on World Wide Web (WWW), 2005, pp. 422–431.

[18] Z. Runfang and H. Kai, "Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing," IEEE Transactions on Parallel and Distributed Systems, vol. 18, no. 4, pp. 460–476, 2007.

[19] B. Li, M. Xing, J. Zhu, and T. Che, "A dynamic trust model for the multi-agent systems," in Proceedings of IEEE International Symposiums on Information Processing (ISIP), 2008, pp. 500–504.

[20] Y. Zhang, S. Chen, and G. Yang, "SFTrust: A double trust metric based trust model in unstructured P2P systems," in Proceedings of IEEE International Symposium on Parallel and Distributed Process- ing (ISPDP), 2009, pp. 1–7.

[21] J. Hu, Q. Wu, and B. Zhou, "FCTrust: A robust and efficient feed- back credibility-based distributed P2P trust model," in Proceedings of IEEE 9th International Conference for Young Computer Scientists (ICYCS), 2008, pp. 1963–1968.

[22] Anupam Das and M. Mahfuzul Islam, "SecuredTrust: A Dynamic Trust Computation
Model for Secured Communication in Multi-Agent Systems," IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING VOL.9 NO.2 YEAR 2012.

[23] D. Wen, W. Huaimin, J. Yan, and Z. Peng, "A recommendation- based peer-to-peer trust model," Journal of Software, vol. 15, no. 4, pp. 571–583, 2004.

[24] J. Sabater and C. Sierra, "Regret: A reputation model for gregarious societies," in Proceedings of the Fourth Workshop on Deception, Fraud and Trust in Agent Societies, 2001, pp. 61–69

[25] Jordi Sabater and Carles Sierra, "Social regret, a reputation model based on social relations," ACM SIGecom Exchanges - Chains of commitment, vol. 3, pp. 44–56, December 2001.

[26] J. Sabater and C. Sierra, "Reputation and social network analysis in multi-agent systems," in Proceedings of the first international joint conference on Autonomous Agents and Multi-Agent Systems, ser. AAMAS '02. ACM, 2002, pp. 475–482.

[27] L. Xiong and L. Liu, "A reputation-based trust model for peer-to- peer ecommerce communities [extended abstract]," in Proceedings of the 4th ACM conference on Electronic commerce(EC), 2003, pp. 228–229.

[28] T. D. Huynh, N. R. Jennings, and N. R. Shadbolt, "An integrated trust and reputation model for open multi-agent systems," Autonomous Agents and Multi-Agent Systems, vol. 13, no. 2, pp. 119–154, 2006.

[29] T. D. Huynh, N. R. Shadbolt, and N. R. Jennings, "Developing an integrated trust and reputation model for open multi-agent systems," in Proceedings of the 7th International Workshop on Trust in Agent Societies, 2004, pp. 65–74.

[30] X. Wang and L. Wang, "P2P recommendation trust model," in Proceedings of IEEE 8th International Conference on Intelligent Systems Design and Applications (ISDA), 2008, pp. 591–595.

[31] L. Wen, P. Lingdi, L. Kuijin, and C. Xiaoping, "Trust model of users' behavior in trustworthy internet," in Proceedings of IEEE WASE International Conference on Information Engineering (ICIE), 2009, pp. 403–406.

[32] Y. Zhang, K. Wang, K. Li, W. Qu, and Y. Xiang, "A time-decay based P2P trust model," in Proceedings of the 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, vol. 2, 2009, pp. 235–238.

BIOGRAPHIES

G.V.Pavan Kumar is student of MallaReddy College of Engineering and Technology, Hyderabad, AP, INDIA. He has received B.Tech Degree Computer Science and Engineering and M.Tech Degree in Computer Science and Engineering. His main research interest includes Networking and Datamining.

J.Praveen Kumar is working as assistant professor in CSE department at Malla Reddy College of Engineering and technology and having 5 years experience in teaching field. Received Post Graduation M.Tech from the stream of Computer Science Engineering from Bharath University Chennai. His main research interest includes Networking and WSN.