ISSN 2348 – 9928
IJAICT Volume 3, Issue 4, April 2016 Doi:01.0401/ijaict.2014.05.12 Published on 05 (4) 2016

INTEGRATED ELLIPTIC CURVE CRYPTOGRAPHY AND FEEDBACK INCENTIVE SCHEME FOR DYNAMIC TRUST MODEL IN MULTI-AGENT SYSTEMS

Ms. P. C. Saranya
Assistant Professor,
Computer Science and Engineering,
Kalaignar Karunanidhi Institute of Technology,
Coimbatore, Tamilnadu, India

Ms. R. Saranya
Assistant Professor,
Computer Science and Engineering,
Kalaignar Karunanidhi Institute of Technology,
Coimbatore, Tamilnadu, India

Abstract— Multi-agent systems are open, anonymous and dynamic in nature. Trust and reputation models fail to properly evaluate the trust of an agent if malicious agents behave in an unpredictable way. These models are ineffective in providing quick response to malicious agent's oscillating behavior and critical for sustaining good service quality .The dynamic trust computation model called Secured Trust analyze different factors related to evaluate the trust of an agent but it fails to address Sybil attack and man in middle attacks. In this paper Elliptic curve cryptography and Feedback Incentive scheme is presented in-order to improve the trust model of multi-agent systems and also the load balancing algorithm is used to improve the quality of service among the service providers. This integrated scheme resists more influential malicious adversaries in the network and also provides efficient distribution of workload among service providing agents under stable condition.

Keywords— Multi-agent System, Trust Management, Reputation Model, Load Balancing, Malicious Behavior.

I. INTRODUCTION

Integrated Public Key Cryptography and Transaction Feedback Incentive (IPKC-TFI) Scheme is used for secured communication as a Dynamic Trust model in Multi-Agent System, Network applications such as pervasive computing, grid computing and P2P networks can be viewed as Multi agent systems which are open, anonymous and dynamic in nature and hence its characteristics introduce vulnerabilities and threats to provide secured communication. In this paper, we consider the integration of public key Cryptography and Transaction feedback incentive (PKE-TFI) scheme to overcome this vulnerabilities and threats. However, the trust models employed by the existing systems do not provide adequate support to coping with quick changes in peers' behavior and aggregating feedback information.

A Reputation-based trust model collects, distributes and aggregates feedback about participants past behavior. These model help agents whom to trust and discourage agents who are dishonest. Most of the global reputation models can successfully isolate malicious agents when the agents behave in a predictable way. However, these models suffer greatly when agents start to show dynamic personality. These models also fail to adapt to the abrupt change in agents behavior and as a result suffer when agents alter their activities. Another aspect which is slowly becoming critical is that proper maintenance of service quality among the trusted service providers.

Secured trust is one of the dynamic trust models which can effectively cope with the dynamic behavior of the malicious agent in the multi agent system but it fails to detect some of the attacks in the network caused by the adversaries. With these research problems in mind, we propose the integrated Public key cryptography and Transaction Feedback incentive (IPKC-TFI) scheme which can effectively cope with the malicious agents behavior in the network and can easily handle the attacks caused by the adversaries by evaluating the trust of the agent. This scheme considers variety of factors in determining the trust of an agent such as satisfaction, similarity, feedback credibility, recent trust, historical trust, sudden deviation of trust and decay of trust and to provide the service quality in the network , workload is distributed evenly among the agents. A new load balancing algorithm is proposed based on approximation of workload present at different service providers.

This model identifies the man in the middle attack using asymmetric encryption scheme and it avoids free ridal problem using feedback incentive scheme. Sybil attack is also identified using this integrated scheme.

II. RELATED WORK

The "Grid problem," which is defined as the controlled and coordinated resource sharing and resource use in dynamic, scalable virtual organizations. "Grid" computing has emerged as an important new field, distinguished from conventional distributed computing by its focus on large-scale resource sharing, innovative applications, and in some cases, high-performance orientation[1]. Trust is a fundamental concern in large-scale open distributed systems. It lies at the core of all interactions between the entities that have to operate in such uncertain and constantly changing environments. The socio-cognitive approach to trust also takes into account the fact that other beliefs about an agent's capabilities and motivations are essential in judging their trustworthiness [2].

The open and anonymous nature of a P2P network makes it an ideal medium for attackers to spread malicious content. In this paper, the model describes a reputation-based trust management protocol for P2P networks where users rate the reliability of parties they deal with, and share this information with their peers. The protocol helps establishing trust among good peers as well as identifying the malicious ones. Results of various simulation experiments show that the proposed system can be highly effective in preventing the spread of malicious content in P2P networks [3].

The model has analyzed as a simple, yet robust method that shows that a solution to this problem is feasible. The trust and reputation mechanisms applied in centralized and decentralized systems. Trust is multi-faceted, even in the same context; agents still need to develop differentiated trust in different aspects of other agents' behaviors [4][5]. Peer-to-peer file-sharing networks are currently receiving much attention as a means of sharing and distributing information. In P2P simulations, using these trust values to bias download has shown to reduce the number of inauthentic files on the network under a variety of threat scenarios [6].

Trust Guard a safeguard framework for providing a highly dependable and yet efficient reputation system [7].Peer-to-Peer (P2P) reputation systems are essential to evaluate the trustworthiness of participating peers and to combat the selfish, dishonest, and malicious peers behavior. The P2P security where servant can keep track, and share with others, information about the reputation of their peers. Reputation sharing is based on a distributed polling algorithm by which resource requestors can assess the reliability of perspective providers before initiating the download. The approach complements existing P2P protocols and has a limited impact on current implementations [9].

A reputation model that takes into account the social dimension of agents and a hierarchical ontology structure that allows considering several types of reputation at the same time. Moreover, the model has to be extended to allow agents to belong to more than one group at a time [10].

III. TRUST AND REPUTATION MODEL

Trust and reputation management has recently become a very useful and powerful tool in some specific environments where a lack of previous knowledge about the system can lead participants to undesired situations, specifically in virtual communities where users do not know each other at all or, at least, do not know everyone. It is in those cases where the application of trust and reputation mechanisms is more effective, helping a peer to find out which is the most trustworthy or reputable participant to have an interaction with, preventing thus the selection of a fraudulent or malicious one.

A Reputation based trust model collects, distributes and aggregates feedback about participants past behaviour and these models help agents decide whom to trust, encourage trustworthy behaviour, and discourage participation by agents who are dishonest Researchers have long been utilizing trust theory from social network to construct trust models for effectively suppressing malicious behaviors of participating agents. Trust issues have become more and more popular since traditional network security approaches such as the use of fire wall, access control, and authorized certification cannot predict agent behavior from a "trust" viewpoint. Reputation-based trust models are basically divided into two categories based on the way information is aggregated from an evaluator's perspective [11].

They are "Direct/ Local experience model" and "Indirect/Global reputation model" where direct experience is derived from direct encounters or observations and indirect reputation is derived from inferences based on information gathered indirectly. Global Reputation Models, an agent aggregates feedback from all the agents who have ever interacted with the target agent, which is an agent has a view of the network which is wider than its own experience, thus enabling it to quickly converge to a better decision [12].

Most of the existing global reputation models can successfully isolate malicious agents when the agents behave in a predictable way.

However, these models suffer greatly when agents start to show dynamic personality. The Trust and Reputation models making an explicit use of other participants' recommendations

IV. INTEGRATED PUBLIC KEY CRYPTOGRAPHY AND TRANSACTION FEEDBACK INCENTIVE (IPKC-TFI) SCHEME

The proposed work called Integrated Public Key Cryptography and Transaction Feedback Incentive scheme for Dynamic Trust Model in Multi Agent Systems for secured communication. Multi-agent systems are open in nature and hence these characteristics introduce vulnerabilities and threats in the network. To minimize the threats, This integrated scheme evaluate the trust of an agent by analyzing various factors related to evaluate the trust of an agent and is effective in providing quick response to malicious agent's oscillating behavior in the network. In-order to provide the quality of service workload is distributed evenly among the service providers by using load balancing algorithm load-balancing algorithm. In addition authentic access control technique is applied to defend Sybil attack and also the data transmission capability is improved in the network.

The phases involved in the proposed scheme are:

- Multi-Agent System and Agent Behavior
- Feedback based Dynamic Secured Trust
- Trust Agent Load Balancing
- Public key cryptography Against Tampering
- Transaction Feedback Incentive

4.1 Multi-Agent System and Agent Behavior

Multi-agent system (MAS) is open and dynamic in nature. Agents interact with each other to achieve a definite goal. Agents are normal or malicious. Multi-agent Systems needs to provide secure information transaction among the agents.. Trust and reputation model ensure effective interactions among participating agents. Trust models are based on social network, Suppress malicious behaviors of participating Agent.

4.2 Feedback based Dynamic Secured Trust

Detect sudden strategic alteration in malicious behavior by evaluating the trust of agents even in highly oscillating malicious activity. Factors determined for trust valuation of an agent are satisfaction, similarity, feedback credibility, recent trust, historical trust, sudden deviation of trust, and decay of trust. Exponential averaging function is used to reduce storage overhead in computing the trust of agents. Feedback credibility measures, degree of accuracy of feedback information that the recommending agent provides to the evaluator. Also it determines the reliability of the feedback. During trust evaluation, feedbacks provided by agents with higher credibility are trust worthier, weighted more than from agents with lower credibility.

4.3 Trust Agent Load Balancing

Calculate a heuristic value of workload. Choose an agent with smallest load or make probabilistic choice based on computed trust value of agents. Classify responders (agents respond to transaction request) based on value of trust threshold as Good service providers (G) and Unknown service providers. Initially, all service providing agents, classified as unknown service providers , as their trust values did not reached a stable state due to lack of transactions. Seek to choose an agent by computing an approximate value (heuristic value) of load present at each responder. Sorting the responders in increasing order of load. Take the responder with smallest workload. In case of no responders present in the class, select an agent either probabilistically based on its trust value or randomly.

Algorithm 1 : Selection of service providing agent(p, S)

Input: *Evaluating agent* ***p*** *and the set of agents responding to a service request* **S.**

Output: *Service providing agent* **q.**

```
for each x € S do
compute Trust (p, x)
if Trust (p, x) > צ then
G < — G U {x}
        Else
U< —— U U {x}
        end if
        end for
if G≠0 then
for each x € G do
```

```
   compute load N(p,x)
        end for
 sort G in increasing order of load N
 return agent q with the smallest  load N
        else
  Total trust < —  0
  for each x € U do
 Total trust < — Total trust +Trust(p,x);
        end for
  if Total trust > 0 then
  for each x € U do
compute Prob(p, x)
        end for
  return agent q with probability  Prob(p, q)
        else
return any agent q randomly
        end if
        end if.
```

4.4 Public key cryptography Against Tampering

Public Key Infrastructure (PKI) uses asymmetric key encryption. Every agent needs to be authenticated creates a key-pair, consisting of a public and a private key. Keys have the property that data encrypted with one key can be decrypted by the other. Given one key, it is computationally infeasible to derive the other key.

Every agent publishes its public key to the multi-agent system, but keeps its own private key as private. Identity of an agent is verified by checking whether an agent (tampers) correctly decrypt a message encrypted with agent's public key. Only real owner of public-private key pair can decrypt the message assuming private key has been kept private. Public key is indeed the public key of the correct agent (or tampering agent) and not of an malicious agent, agent using its own generated key pair is the task of the PKI.

4.5 Transaction Feedback Incentive

In this Untrustworthy feedback is ignored and old feedback values are discounted over time. Outcome of transaction is measured with three different kinds of reputation. Transaction Feedback Incentive measure incentive values on secured trust model. Incentive factor is proportional to the ratio of total feedbacks over transactions. Initiate authenticated access control with incentive factors thwart Sybil attack. With feedback incentive on transaction of information, structural changes of identity and community are restricted. Exit and entry with a new identity become difficult to gain incentive value on transaction and lost its reputation.

V. CONCLUSION

The integrated public key cryptography and Transaction Feedback Incentive Scheme Provides an efficient load balancing algorithm in which the performance is improved by Sybil attack rate and data transmission rate. The malicious agents are identified effectively by evaluating the trust of an agent based on various factors.

References

[1] Anupam Das , Mohammad Mahfuzul Islam ,"A Dynamic Trust Computation Model for Secured Communication in Multiagent Systems", IEEE Transactions on dependable and secure computing, vol. 9, no. 2, march/april 2012.

[2] 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, 2004.

[3] 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, 2004.

[4] K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-Peer Information System," Proc. 10th Int'l Conf. Information and Knowledge Management (CIKM '01), pp. 310-317, 2001.

[5] Y. Wang and J. Vassileva, "Bayesian Network-Based Trust Model,"Proc. IEEE/WIC Int'l Conf. Web Intelligence (WI '03), pp. 372-378 Oct. 2003.

[6] S.D. Kamvar, M.T. Schlosser, and H. Garcia-Molina, "The EigenTrust Algorithm for Reputation Management in P2P Networks," Proc. 12th ACM Int'l World Wide Web Conf. (WWW '03), pp. 640-651, 2003.

[7] M. Srivatsa, L. Xiong, and L. Liu, "TrustGuard: Countering Vulnerabilities in Reputation Management for Decentralized Overlay Networks," Proc. 14th ACM Int'l Conf. World Wide Web (WWW '05),

[8] Z. Runfang and H. Kai, "PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing," IEEE Trans.Parallel and Distributed Systems, vol.18, no. 4, pp. 460-473, Apr. 2007.

[9] E. Damiani, S.D. Capitani, S. Paraboschi, and P. Samarati, “Managing and Sharing Servants’ Reputations in P2P Systems,” IEEE Trans. Knowledge and Data Eng., vol.15, no.4, pp.840-854, July/Aug. 2003.

[10] J. Sabater and C. Sierra, “REGRET: A Reputation Model for Gregarious Societies,” Proc. Fourth Workshop Deception, Fraud and Trust in Agent Societies, pp. 61-69, 2001.

[11] Brajesh Patel, Neha Jha , “Elliptic Curve Cryptography in Networks with Hidden Generator Point for Speedup Scalar Multiplication” IJMIE Volume 2, Issue 6 June 2012 .

[12] Miriam Heitz, Stefan König, Torsten Eymann, “Reputation in Multi Agent Systems and the Incentives to Provide Feedback”, Lehrstuhl für Wirtschaftsinformatik Universität Bayreuth September 2010.