IJCAT International Journal of Computing and Technology, Volume 1, Issue 2, March 2014
ISSN : 2348 - 6090
www.IJCAT.org

A Survey on Trust Management in Peer to Peer Systems

[1] Manju John, [2] Govindaraj.E

[1] Computer Science and Engineering, MES College of Engineering, Kuttippuram, Kerala, India

[2] Computer Science and Engineering, MES College of Engineering, Kuttippuram, State, Kerala, India

Abstract - Trust management in P2P system is used to detect malicious behaviors and to promote honest and cooperative interactions. The main goal of the earlier P2P systems is the capability of aggregating resources, which assumes certain honesty level of peers. However, as P2P systems grow tremendously in size, there will be a considerable number of malicious peers who bring security attacks and threats to the whole network. In a distributed infrastructure without centralized server for authority, providing security mechanism is more complicated than in server-centric solutions, as the existence of multiple sites increases the vulnerability and security efforts must be replicated at multiple sites. Therefore security issues are one of the major challenges that need to be carefully analyzed and addressed, especially for fully decentralized unstructured P2P systems. A lot of researches are being conducted to improve the trust management in peer to peer system. Several reputation-based trust management systems are analyzed here.

Keywords **- Peer-to-peer computing, reputation system, PGrid, Eigen Trust, Peer Trust, Gossip Trust, Power Trust, TMS, SORT.**

1. Introduction

Peer to peer (P2P) systems rely on collaboration of peers to accomplish tasks. Ease of performing malicious activity is a threat for security of P2P systems. Creating long-term trust relationships among peers can provide a more secure environment by reducing risk and uncertainty in future P2P interactions. Particularly trust management systems are classified into three categories, reputation-based trust systems, policy-based trust systems, and social network-based trust systems. Reputation is a measure that is derived from direct or indirect knowledge on earlier interactions of agents, and it is used to access the level of trust an agent puts into another agent. Thus, reputation-based trust management is one specific form of trust management. Reputation-based trust management systems on the other hand provide a mechanism, by which a peer requesting a resource may evaluate the trust in the reliability of the resource and the peer providing the resource. The goal of this survey is to analyze the researches on the P2P reputation-based trust management

2. Literature Survey

Malicious peers have more attack opportunities in P2P trust models due to lack of a central authority. Researches are always being conducted to improve the accuracy and efficiency of the trust management in peer-to-peer systems. Some of the innovative approaches are described.

2.1 DMRep

On a structured P2P system, a DHT structure can provide decentralized and efficient access to trust information. In Aberer and Despotovic's trust model [1], peers report their complaints by using P-Grid. It is an approach that addresses the problem of reputation-based trust management at both the data management and the semantic level. A peer is assumed as trustworthy unless there are complaints about it. However, preexistence of trust among peers does not distinguish a newcomer and an untrustworthy one.

The principal advantage of this approach is that it has an efficient way of storing and retrieving trust data and does not flood every peer in the system with queries about other peers, thus limiting storage and bandwidth costs. It is thus more scalable than approaches that broadcast trust queries to all peers in the system.

The main disadvantage, however, is that a peer is forced to store data owned by other peers and does not have local control over the treatment of that data. Therefore, the system is not truly decentralized because peers have to

implicitly agree to not alter data owned by others. It also does not employ any kind of mechanism to authenticate messages or explicitly protect the identity of peers. And DMRep assumes that usually trust exists and malicious behaviour is the exception, thus it is not suitable for the environment with high cheating rates.

2.2 Eigen Trust

Eigen Trust [2] uses transitivity of trust to calculate global trust values stored on CAN. The basic idea of secure algorithm is that the trust value of one peer is computed by some other peers. Those peers are called mothers which are responsible for computing their daughter's global reputation values. The reason for using more than one other peer to compute a peer's reputation value is that some mothers may be malicious peers and they report false trust values for their daughters. Hash functions map a Unique ID for each peer (IP Address and TCP port) into points in a logical coordinate space. Coordinate space is partitioned over the network and every peer covers a region of that dynamic space. The peer who covers the region where that ID is hashed becomes that peers score manager.

Advantages of Eigen Trust are (1) Isolate malicious peers by using multiple mothers to calculate and store reputation values for a peer. (2) Encourage peers to share file by rewarding reputation to those peers which provide good services. (3) Allow the new peers to build trust (4) Balance the load by downloading probabilistically so that low reputation peers still have chance to be selected.. And its disadvantages includes (1) Cannot distinguish between newcomers and malicious peers (2) Malicious peers can still cheat in collectives (3) The flexibility of calculating global reputation value (4) Anonymous. That is it is not possible for a peer at a specific coordinate to find out which peer ID exactly it computes for.

2.3 Peer Trust

Peer Trust [4] defines transaction and community context parameters to make trust calculation adaptive on P-Grid. The parameters are:

- The feedback a peer obtained from others
- The feedback scope
- Credibility factor for the feedback source
- The transaction context factor

While transaction context parameter addresses application dependent factors, community context parameter addresses P2P community related issues such as creating incentives to force feedbacks. As an advantage we can say peer trust is a coherent adaptive trust model for quantifying and comparing the trustworthiness of peers. Also peer trust identifying five important factors for evaluating the trust and minimize security weakness and prevents man in the middle attack.
However one important disadvantage is peers can easily discard their old identity and adopt a new one through re-entry to get rid of bad history. And also a peer can perform an unavoidable one-time attack.

2.4 Power Trust

Power Trust [5] constructs an overlay network based on the Power law distribution of peer feedbacks. It dynamically selects small number of power nodes that are most reputable using a distributed ranking mechanism. A reputation system calculates the global reputation score of a peer by considering the feedback from all other peers who have interacted with this peer. A trust overlay network is used to model the trust relationship among peers. The community context factor by using a random-walk strategy and utilizing power nodes, feedback aggregation speed, and global reputation accuracy are improved. Advantage of power trust includes power law distribution of peer feedbacks, fast reputation aggregation, ranking, updating, system robustness and operational efficiency. And disadvantages are (1) Power trust cannot be deployed on unstructured networks (2) Does not deal with intrusions, collusions, and selfishness of peers (3) Calculated trust information is not global and does not reflect opinions of all peers

2.5 Gossip Trust

Gossip Trust [6] defines a randomized gossiping protocol for efficient aggregation of trust values. A query is randomly forwarded to some neighbours instead of all neighbours. Comparing to flooding approach, gossiping reduces reputation query traffic. Gossip protocol tolerates the network link and node failures and support the computation of aggregate functions like weighted sum, average value and maximum over large collection of distributed numeric values One thread sends the halved gossip pair 1/2 x(k), 1/2 wi(k) to itself (node i) and to a randomly selected node in the network. Another thread receives all halved pairs from other nodes and computes the updated xi(k+1) and wi(k+1) xi is the gossiped global score and wi is the gossiped weight Gossip Trust is an extension of gossip protocol. It uses the gossip protocol to aggregate reputation scores. It treats all opinions in gossip procedure with the same weight regardless of the sources of the opinions. Gossip trust is a fast gossip-based

reputation aggregation algorithm with small aggregation error. It has efficient reputation storage with Bloom filters with low false-positive error. It uses power nodes dynamically for combating against peer collusions. But Gossip trust is not suitable for large P2P networks, only tested on small simulations and does not have been implemented in real world.

2.6 Trust Management System (TMS)

A partially decentralized reputation-based TMS [8] for BitTorrent is presented which uses global trust scores to evaluate peers as well as their local trust scores. It uses the BitTorrent peers transactions for calculating local scores and the BitTorrent tracker to compute global trust scores. Peers calculate and assign local score to each other. Then peers send these local scores to the tracker. Tracker calculates global score of peers and find top 10 percent of peers. These 10 percent of peers determine global score of the other peers. Global scores return back to the peers. TMS can reach a steady state during early phases of its life. Thus, the TMS can prevent rogue peers to be selected as Super-Peer. The main threat for the proposed TMS is collusion attack. Relying on the tracker to calculate the global trust scores, adds overhead to the tracker when the size of the swarm is extremely large.

2.7 SORT

Ahmet Burak Can and Bharat Bharagava et al. [7] propose a Self-ORganizing Trust model (SORT) aims to decrease malicious activity in a P2P system by establishing trust relations among peers in their proximity. No a priori information or a trusted peer is used to leverage trust establishment. Peers do not try to collect trust information from all peers. Each peer develops its own local view of trust about the peers interacted in the past. In this way, good peers form dynamic trust groups in their proximity and can isolate malicious peers. SORT defines two context of trust, service and recommendation contexts are defined to measure capabilities of peers in providing services and giving recommendations. Interactions and recommendations are considered with satisfaction, weight, and fading effect parameters. A recommendation contains the recommenders own experience, information from its acquaintances, and level of confidence in the recommendation.

In SORT instead of global trust information local trust information is enough to make decisions. Peers send reputation queries only to peers interacted in the past which reduces network traffic and make simulations realistic.Disadvantages are if a peer changes its point of attachment to the network, it might lose a part of its trust network and it does not solve all security problems but enhance security and effectiveness of the system.

Table 1: Performance Analysis

Trust Management System	P2P type	Local Trust Evaluation	Global Trust Evaluation	Data Management
DMRep	Structured	Binary Trust	Using complaints	P Grid
Eigen Trust	Structured	Sum of positive and negative ratings	Using pre-trusted peers	DHT (Distributed Hash Table)
Peer Trust	Structured	Normalized rating on each transaction	Calculates trust score using five factors	P Grid
Power Trust	Structured	Using Bayesian method	Using power nodes and LRW strategy	TON (Trust Overlay Network)
Gossip Trust	Structured and Unstructured	Using Bayesian method	Gossip based protocol	Bloom filter storage
TMS	Structured	Considers peer's co-operation with download and upload parameters	Using super peers	Bit-Torrent network
SORT	Structured and Unstructured	Considers both feedback and recommendations	-	

3. Performance Analysis

Table 1 compares the reputation-based trust management systems in four technical aspects:

.

4. Conclusions

Open nature of peer-to-peer systems exposes them to malicious activity. Building trust relationships among peers can mitigate attacks of malicious peers. Reputation-based trust management is used to pro- mote honest and cooperative behaviors, and thus the overall credibility of the P2P network can be maintained at an expected level. Various methods for trust management in peer to peer systems have been compared. Each methods have its own merits and demerits. Solutions on a structured network rely on a DHT structure to store trust information. Each peer becomes a trust holder of another peer, which is assumed to provide authentic global trust information. A number of issues for future studies remain open. First, more extensive evaluation methods over wider parameters are needed. Second, robust methods are needed to avoid the malicious peers cheat in collectives, as the current works are based on the assumption that the probability of cheating within a society is comparably low.

References

[1] K. Aberer and Z. Despotovic, Managing Trust in a Peer-2- Peer Information System, Proc. 10th Intl Conf. Information and Knowledge Management (CIKM) 2002.

[2] S. Kamvar, M. Schlosser, and H. Garcia-Molina, The (Eigentrust) Algorithm for Reputation Management in P2P Networks ,Proc. 12th World Wide Web Conf. (WWW) 2002.

[3] [3] F. Cornelli, E. Damiani, S.C. Vimercati, S. Paraboschi, and P. Samarati, A reputation-based approach for choosing reliable resources in peer-to-peer networks ,In CCS02, Washington DC, USA 2002.

[4] L. Xiong and L. Liu, Peertrust: Supporting Reputation-Based Trust for Peer-to-Peer Ecommerce Communities, IEEE Trans. Knowledge and Data Eng., vol. 16, no. 7, pp. 843-857 July 2004.

[5] R. Zhou and K. Hwang, 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.

[6] R. Zhou, K. Hwang, and M. Cai, Gossiptrust for Fast Reputation Aggregation in Peer-to-Peer Networks, ,IEEE Trans. Knowledge and Data Eng., vol. 20, no. 9, pp. 1282-1295, Sept. 2008.

[7] Behrooz Shafiee Sarjaz Maghsoud Abbaspour, BitTorrent using a new reputation-based trust management system, Springer Science+Business Media Sept. 2012.

[8] Ahmet Burak Can, Member, IEEE, and Bharat Bhargava, Fellow, IEEE, SORT: A Self-ORganizing Trust Model for Peer-to-Peer Systems, IEEE Transactions on Dependable and Secure Computing, vol. 10, NO. 1, Feb. 2013.

[9] Ankur Gupta, Peer-to-peer networks and computation: Current trends and future perspectives, Computing and Informatics, Vol. 30, 559594, 2011.

[10] Kevin Hoffman, David Zage, and Cristina Nita-Rotaru, A Survey of Attack and Defense Techniques for Reputation Systems,Proc.16th ntl World Wide Web Conf. (WWW 07), 2009.

Manju John received the bachelor's degree in Computer Science and Engineering from Mahatma Gandhi University, Kerala in 2012. Presently she is pursuing her M.Tech in the department of Computer Science and Engineering from University of Calicut, Kerala. Her research interests include computer networks, trust in peer to peer networks etc.

Govindaraj E received the bachelor's degree in Computer Science and Engineering from the University of Calicut, Kerala and master's degree and PhD in Computer Science and Engineering from Anna University, Tamil Nadu. Currently he is working as an Associate Professor in Computer Science and Engineering Department, MES College of Engineering, under Calicut University Kerala. He has teaching experience of eight years. His research interests include computer networks, wireless sensor networks etc.