ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Establishing trust relationship in peer to peer systems

M.Pratyusha
M.Tech Student,
Department of CSE,
Aditya Engineering College,
Surampalem, Kakinada, E.G D.t, A.P, India.

N.Siva Kumar
Sr. Asst. Professor,
Department of CSE,
Aditya Engineering College,
Surampalem, Kakinada, E.G D.t, A.P, India.

Abstract:

Peers collaborate to establish trust among each other without using a priori information or a trusted third party. A peer's trustworthiness in providing services, e.g., uploading files, and giving recommendations is evaluated in service and recommendation contexts. Three main trust metrics, reputation, service trust, and recommendation trust, are defined to precisely measure trustworthiness in these contexts. An interaction is evaluated based on three parameters: satisfaction, weight, and fading effect. When evaluating a recommendation, including to these parameters, recommender's trustworthiness and confidence about the information provided are considered.

A file sharing application is simulated to understand capabilities of the proposed algorithms in mitigating attacks. For realism, peer and resource parameters are based on several empirical studies. Service and recommendation based attacks are simulated. Nine different behavior models representing individual, collaborative, and identity changing malicious peers are studied in the experiments. Observations demonstrate that malicious peers are identified by good peers. The attacks are mitigated even if they gain high reputation.

Collaborative recommendation-based attacks might be successful when malicious peers make discrimination among good peers. Identity changing is not a good attack strategy.The objective of the work is to prevent peer-to-peer systems exposes them to malicious activity. Building trust relationships among peers can mitigate attacks of malicious peers. This paper presents distributed algorithms that enable a peer to reason about trustworthiness of other peers based on past interactions and recommendations.

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.

However, establishing trust in an unknown entity is difficult in such a malicious environ-ment. Furthermore, trust is a social concept and hard to measure with numerical values. Metrics are needed to represent trust in computational models. Classifying peers as either trustworthy or untrustworthy is not sufficient in most cases. Metrics should have precision so peers can be ranked according to trustworthiness.

Interactions and feedbacks of peers provide information to measure trust among peers. Interactions with a peer provide certain information about the peer but feedbacks might contain deceptive information. This makes assessment of trust-worthiness a challenge.

We propose a Self-ORganizing Trust model (SORT) that enables peers to create and manage trust relationships without using a priori information. Since preexistence of trust among peers does not distinguish a newcomer and a trustworthy one, SORT assumes that all peers are strangers to each other at the beginning. Peers must contribute others in order to build trust relationships.

Malicious behavior quickly destroys such a relationship. Thus, Sybil attack that involve changing of pseudonym to clear bad interaction history is costly for malicious peers.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

In SORT, trusted peers are not needed to leverage trust establishment. A trusted peer can not observe all interactions in a P2P system and might be a source of misleading information. A peer becomes an acquaintance of another peer after providing a service to it, e.g., uploading a file. Using a service from a peer is called a service interaction. A recommendation represents an acquaintance's trust information about a stranger. A peer requests recommendations only from its acquaintances. Measuring trust using numerical metrics is har. Classifying peers as either trustworthy or untrustworthy is not sufficient. Metrics should have precision so peers can be ranked according to their trustworthiness .

As in Eigentrust, SORT's trust metrics are normalized to take real values between 0 and 1. Eigentrust counts two peers equally trustworthy if they are assigned to the same trust value. In SORT, trust values are considered with the level of past experience. A peer with more past interactions is preferred among peers assigned to the same trust value. The intuitive notion of "dependability" for these systems is one of reachability of information. Accordingly, dependability should be measured by the percentage of times that a request results in the proper information moving from its source(s) to its destination(s).

The requirements for dependability vary greatly within the parameter space of P2P systems. Consider a point-to-point system designed to answer existence queries. An instance where every node has a completely up-to-date and accurate picture of the rest of the system and where the bandwidth consumed by queries and state transfer does not exceed the capacity of any links would be perfectly dependable. However, such a design might not work if the type of information exchanged was event-driven: if, for example, one node needed to notify another node or collection of nodes when there was an abrupt temperature change or if a bridge were about to collapse.

In this paper, we define dependability in P2P systems and discuss the way in which Chord and our own hierarchically grouped system self-organize to overcome the unreliability of nodes that comprise the system.

Reliability in Decentralized Systems:

A system's dependability is defined in terms of three characteristics: the type and method of information exchange (e.g., probes, point-to-point streams, broadcast streams, etc.), the individual nodes' capabilities, and the distribution of data and queries among the nodes. One thread links all three components: local information must provide a quantifiable and probabilistically accurate depiction of the global state. The required level of this accuracy depends on system usage; increased tolerance for out of date local information leads to diminished state, messages, bandwidth, and uptime requirements.

For example, in Chord, the likelihood that requests will be fulfill-able depends on the join/failure rate and on the rate at which a node ring stabilization procedure is run, which in turn depends on the node's capacity for topology messages. Trust models on P2P systems have extra challenges comparing to e-commerce platforms. Malicious peers have more attack opportunities in P2P trust models due to lack of a central authority. Hoffman et al. discuss five common attacks in P2P trust models: self promoting, white-washing, slandering, orchestrated, and denial of service attacks.

They point out that defense techniques in trust models are dependent to P2P system architecture. On a structured P2P system, a DHT structure can provide decentralized and efficient access to trust information. In Aberer and Despotovic's trust model , peers report their complaints by using P-Grid .

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. Eigentrust uses transitivity of trust to calculate global trust values stored on CAN. Trusted peers are used to leverage building trust among regular peers and mitigate some collaborative attacks.

PeerTrust defines transaction and community context parameters to make trust calculation adaptive on P-Grid. While transaction context parameter addresses application dependent factors, community context parameter addresses P2P community related issues such as creating incentives to force feedbacks.

The first component to the overall dependability of a decentralized system is the type of information exchanged across it. We divide information exchange into the following five categories:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

PROBE :

Probe queries test for the existence of an object. These queries often use a filter structure (e.g., DHTs or Bloom filters) or resource intensive naive broadcast queries the latter gives the significant advantage of high tolerance against node failure and allows for receiver-interpreted queries.

event-driven point-to-point:

A node registers an interest and is contacted when something matching this interest enters the system. Examples include abrupt temperature change, sensor aggregators , change in file contents, file creation, new authorship, and distributed triggers.

event-driven broadcast :

This is a broadcast from one node to all other nodes, used to distribute information globally. This could be used, for example, to implement a software update.

continuous stream point-to-point :

This exchange provides a path for streaming data for an indeterminate duration to another node or other nodes. Internet routing is one such example. The requirement of continuity may mean pro-active measures against unknown failures will be necessary (e.g. using multiple paths), compared with just post-failure cleanup and recovery.

continuous stream broadcast:

One node continuously updates the entire system, similar to continuous stream point-to-point. The ubiquitous nature of this type of exchange may make it much easier to implement in P2P systems without pro-active routine measures.

Terminology from the fault tolerant community can be misleading when applied to distributed decentralized systems. Mean-time-to-failure here refers to the mean-timeto- node-departure. Mean-time-to-data-loss has less meaning when nodes are always entering and exiting the system; queries always have a significant chance of failing under realistic conditions.

For P2P filesharing systems we can define mean-time-to-query-failure (MTQF). More generally, the dependability can be quantified by the mean-time-torequest-failure (MTRF), which allows for all five categories of information exchange to be considered.

Hierarchy Structure:

We define the ideal topology as a collection of groups of nodes, where the nodes in a group are related based on low intra-group latency and varied mean-time-to-failure (MTTF), and heterogeneous bandwidth. Our goal is to come as close to this ideal topology as possible using only local information. Nodes benefit from being in a group because they share information about other groups filter. These benefits increase as groups grow in size. Nodes also benefit from the existence of other groups, because transmitted group summaries serve as an efficient mechanism to prune the search space.

RELATED WORK:

A formal model of trust based on sociological foundations is defined by Marsh . In this model, an agent uses own experiences when building trust and does not consider information of other agents. Abdul-rahman and Hailes' trust model evaluates trust as an aggregation of direct experience and recommendations of other parties. Trust metrics are defined in discrete domain. A semantic distance measure is defined to test accuracy of recommendations.

Zhong proposes a dynamic trust concept based on McKnight's social trust model . Uncertain evidences can be used when building trust relationships. Second-order probability and Dempster- Shaferian framework helps in evaluating uncertain evidences.Methods are proposed as countermeasures.

Despotovic and Aberer study an online trade scenario among self-interested sellers and buyers. Trust-aware exchanges can increase economic activity since some exchanges may not happen without trust establishment. Terzi et al.introduces an algorithm to classify users and assign them roles based on trust relationships. Yu and Singh's model propagates trust information through referral chains.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Referrals are the primary method of developing trust in others. Mui et al.propose a statistical model based on trust, reputation and reciprocity concepts. Reputation can be propagated through multiple referral chains. Jøsang et al. discusses transitivity of trust with referrals. Recommendations based on indirect trust relations may cause incorrect trust derivation. Thus, trust topologies should be carefully evaluated before propagating trust information.

Larger groups provide more shared information, but this benefit is offset by the cost of keeping the group reasonably balanced, maintaining group summaries, and the load on the root. The root's workload grows with the size of the group as it will broker all group searches, maintain group and child summaries, control entry to the group and determine the time for partitioning of the group. It is this last responsibility, determining partition time, that makes the system feasible. When the root becomes overloaded, it sheds load by partitioning the group.

This partitioning, in conjunction with responding to requests to join the group, is what provides the dynamism and selfconfigurability of the system.Several other projects have proposed "supernodes" as the solution to the heterogeneity empirically extant in P2P systems. Saroiu et al. have shown that there are multiple, distinct categories of nodes, ranging from always-on highbandwidth nodes to 56k modems only connected for an hour or less. Hierarchies form a good extension to the "supernodes" currently proposed in several research projects (e.g., Gnutella++ [8], Brocade [26]). In these projects, thereare two levels of nodes: "supernodes" that do most of the routing, and regular nodes. A more general heterogeneous system should use a heterogeneous topology, with "better" nodes living closer to the root of each group.

Grouping Analysis:

We base our grouping model on natural systems that exhibitself-configuration, driven by particle interactions thatlower energy costs when an organized state is realized. Evolutionmodels [2], non-equilibrium phase transitions [24],and crystal facet structure formation [15] among others, allshow this behavior, and these ideas have been widely appliedto a number of economics and engineering problems.

We derive a node's cost based on its bandwidth consumption,though a refinement to include latency would be a naturalextension of this method. To make grouping decisions,nodes compare their current cost with the cost of being inthe other groups of which they are aware. If, by forming agroup, two nodes can lower the number of queries they receiveand the efficiency of the queries they generate, then agroup configuration is more desirable. However, there is anactivation cost to form a new group, comprised of the onetime cost of distributing filters and reorganizing the tree. Ifgroups only form when the cost of the old state exceeds thesum of the activation cost and the new state's cost, we canencourage stability.

Having groups flit in and out of existenceis expensive and is mitigated by this activation cost.As noted above, the overall cost that each node seeks tominimize is the weighted sum of the bandwidth costs. Bandwidthusage consists primarily of queries and filter updates. We assume nodes have poor knowledge of the system outsidetheir own group, making query estimates difficult. Theonly reliable computation nodes can perform with regards tothe costs outlined above are those local to the group, that is,specific to the filters. We set the individual group filter costto the fraction of bandwidth consumed by filter messages to total bandwidth.

Conclusion:

This paper makes three contributions. First, we examine how the implicit goals and assumptions about a particular decentralized system affect measures of its reliability. Second, we introduce a self-organizing hierarchically-based P2P system. Third, we take the assumptions implicit in current P2P filesharing systems and evaluate the reliability of Chord and the hierarchical grouping system. In simulation experiments, both systems perform adequately as long as there exist a percent tolerance for failure under normal conditions.

This failure rate is probably acceptable for a file sharing situation but would need to be tampered by a higherlevel application that would provide redundancy in more rigorous file system-like scenarios. Both systems utilize selfconfiguration stabilize and local-information-based group formation — to maintain an adequate degree of reliability even under high fluctuation.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

In particular, our model enables the formation of local points of stability and high bandwidth, and we show how self-configuration can create many local foci to which the rest of the more dynamic system can attach.

REFERENCES:

[1] K. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-Peer Information System," Proc. 10th Int'l Conf. Information and Knowl-edge Management (CIKM), 2001. ||

[2] F. Cornelli, E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Samarati, "Choosing Reputable Servents in a P2P Network," Proc. 11th World Wide Web Conf. (WWW), 2002. ||

[3] S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The (Eigentrust) Algorithm for Reputation Management in P2P Networks," Proc. 12th World Wide Web Conf. (WWW), 2003. ||

[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] A.A. Selcuk, E. Uzun, and M.R. Pariente, "A Reputation-Based Trust Management System for P2P Networks," Proc. IEEE/ACM Fourth ||

[6] Int'l Symp. Cluster Computing and the Grid (CCGRID), 2004. ||

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

[8] J. Kleinberg, "The Small-World Phenomenon: An Algorithmic Perspective," Proc. 32nd ACM Symp.Theory of Computing, 2000. ||

[9] S. Saroiu, P. Gummadi, and S. Gribble, "A Measurement Study of Peer-to-Peer File Sharing Systems," Proc. Multimedia Computing and Networking, 2002. ||

[10] M. Ripeanu, I. Foster, and A. Iamnitchi, "Mapping the Gnutella Network: Properties of Large-Scale Peer-to-PeerSystems and Implications for System Design," IEEE Internet Computing, vol. 6, no. 1, pp. 50-57, Jan. 2002. ||

[11] S. Saroiu, K. Gummadi, R. Dunn, S.D. Gribble, and H.M. Levy, "An Analysis of Internet Content Delivery Systems," Proc. Fifth USENIX Symp.Operating Systems Design and Implementation (OSDI), 2002. ||

Author Details:

Miss.M.Pratyusha

is a student of Aditya Engineering College, Surampalem. Presently she is pursuing her M.Tech [CSE] from this college and she received her B.Tech degree in Computer Science and engineering from Chaitanya Institute of Engineering and Technology, affiliated to JNTU Kakinada in the year 2012.Her area of interest includes Computer networks, Object oriented languages and current trends in Computer Science.

N.siva kumar

obtained B.Tech in computer science and enginnering from kakinada inistitute of engineering and technology affliated to jntuh hyderabad..studied M.Tech in computer science from aditya engineering college affliated to jntuk kakinada. Presently working as assistant professor in computer science & engineering college surampalem.my intrested areas networks..compiler design. Formal languages and automata theory.