Secure Data and Service Access Model for Peer-to-Peer Systems using Trust Relations

Sourabh S. Mahajan
PG student, Computer Department
Smt. Kashibai Navale College of Engineering, Pune

S.K. Pathan
Assistant Professor, Computer Department
Smt. Kashibai Navale College of Engineering, Pune

ABSTRACT
Peer-to-Peer systems are based on collaboration of peers to accomplish tasks. Trust relationship among peers can help to reduce attacks of peers with malicious intent. In this paper we presents algorithms which helps a peer to reason about trustworthiness of other peers based on interactions in the past and recommendations. Peers create trust network using local information and does not need to deal with global information. Service and recommendation metrics describes the trustworthiness of peers in providing services. Recentness, importance and peer satisfaction parameters are considered for evaluating interactions and recommendations. A good peer can isolate malicious peers with the help of trust relationships.

General Terms
Peer-to-peer systems, self organized network, trust relations, security.

Keywords
Recommendations, trustworthiness

1. INTRODUCTION
Peer to peer (P2P) systems merges large number of computers that enters or leave network frequently. In peer to peer systems individual machine can communicate with each others and share resources without dealing the central coordinator. Building long term trust relationships provides more secure environment which reduces risk and uncertainty in the future. Metrics are required to describe trust in computational model. Trust among peers is measured based on the information provided by interactions and feedbacks of peers.

The systems such as eBay prefer the central server to store and manage trust information. In most P2P systems central authority is not present to deal with storing and managing trust information about each other [1], [2]. Structure of P2P systems resolves management of trust information. In approaches such as distributed hash table (DHT), feedback storing about other peers which made peer as trust holder [1], [3], [4]. Global trust information is accessed through DHT which is stored by trust holders. A peer sends queries for trust to know trust information of other peers. A query is either flooded to network or to neighbor of query initiator.

Self Organizing Trust model (SORT) decreases malicious intents with the help of trust relationship among peers. Peers does not collect trust information from all peers because each peer develops its local trust about peers interacted in the past, so good peer can isolate malicious peers. At beginning peers are said to be strangers to each other. A peer is said to be acquaintance of another when it provides service e.g.; file uploading. A peer sets to trust stranger when it has no acquaintance. If there is equality in trustworthiness then acquaintance is preferred over stranger. Using a service of a peer is said to be an interaction. It is computed based on recentness of the interaction, weight (importance). Recommendation, which is feedback of acquaintance, is computed based on trustworthiness of recommender. It involves the own experience about the peer of recommender, information from recommender's acquaintances, and recommender's level of confidence. The recommendation has a low value if level of confidence is low, which affects less the trustworthiness of recommender.

SORT defines two context of trust: service and recommendation trust. In these contexts, separate histories are maintained to store information about past interactions and recommendations in order to assess competence and integrity of acquaintances. There are three trust metrics: Reputation metric-It is computed based on recommendations. It considers to be prime when deciding about strangers and new acquaintances. Service trust metric and Recommendation trust metrics are considered in order to measure trustworthiness in the service context and recommendation contexts. Service providers are selected based on service trust metric, whereas recommendation trust metric is used when requesting recommendations. Recommendations are computed based on recommendation trust metric in order to compute reputation metric. SORT deals with the service based attacks as well as recommendation based attacks. SORT describes, good peer can protect themselves against peers with malicious intents without using global trust information, and instead it uses local trust to assess trustworthiness of other peers.

2. LITERATURE SURVEY
There are various models are developed concerning with the protection in peer to peer environment. Marsh [6] employed a formal trust model which is based on sociological foundations. An agent which considers own experience for building trust relations and does not deal with information of other agents. Abdul-rahman and Hailes [7] considers trust in discrete domain as an integration of experience and recommendations of other parties. Yu and Singh's model [8] defines trust information through referral chains. Trust in other is developed by the method named as referral. Mui et al [9] developed statistical model based on trust, reputation, and reciprocity. Terzi et al [10] developed algorithm which classifies users and assign them roles based on trust relationship.

To build trust reputation systems are widely used in e-commerce. A central authority is used to collect past customer's feedback which is used by future customers in shopping decisions. There are more opportunities of attack in P2P trust model for malicious peers due to absence of central coordinator. Attacks in P2P trust model such as self promoting, white washing, slandering, orchestrated, and denial of service attacks discussed by Hoffman et al and they said that defense technique in trust models are dependant to P2P architecture.

DHT structure provides decentralized approach and access to trust information in the structured P2P environment. A peer in Aberer and Despotovic's trust is treated as trustworthy unless there are complaints about it. In Eigntrust [3], global trust values are calculated using trust transitivity. Peer trust [4] describes parameters such as transaction and community context for having trust calculation adaptive on P-grid. Transaction context parameters describe application dependant factors whereas community context parameter exposes P2P community related issues like creating incentives to have feedback. Eigntrust and Peertrust compute recommendations which are based on trustworthiness of the recommender.

Song et al [11] suggests a fuzzy logic trust model that performs same as Eigntrust [13] but with lower message overhead. There are two major steps performed by the fuzzy system: Local score calculation and Global reputation aggregation. In local score fuzzy operations are performed by peers on local parameters to create local score. Fuzzy logic is self adjusting and holds some uncertainties. Local trust scores which are collected from all peers are aggregated by fuzzy system in order to generate global reputation for each peers. Fuzzy inference is used by the system to get global reputation aggregation weights. Aggregation weights are determined by variables named peer's reputation, transaction date and transaction amount. In fuzzy trust system based on DHT, each peer maintains transaction record table and local score table. Transaction record table maintains transaction records with remote peers whereas local score table holds trusted score evaluated by remote peers.

PowerTrust [14] suggests an overlay network which is based on the power law distribution of peer feedbacks. In DHT structure each peer is trust holder of another peer, which is considered to provide authentic global trust information. In SORT public opinion is assumed to be more crucial information instead of dealing with a specific trust holder's feedback as authentic. Local trust information is used to take decisions irrespective of global trust as peer develops their own trust network

Trust queries are broadcasted to whole network in unstructured P2P systems. Corneli et al. floods trust queries in Gnutella network [5] which is self organizing, scalable and having open architecture.Gnutella network stands, at application level, virtual network with routing mechanism. Gnutella achieved reliability, scalability, performance with virtual network and routing mechanism. Gnutella survey determines characteristics of participating resources. It is decentralized mechanism and search protocol, which is used for the purpose of file sharing. Gnutella nodes named servants perform tasks related with server as well as client. Nodes accept queries from other servants match it with local components and generate corresponding result. When nodes are attached to the network, nodes sends message to interact with each other where message can be broadcasted in the network or backpropogated .Virendra et al [12] considers trust concept in mobile ad hoc networks which are used to generate keys among nodes and group nodes. Feedbacks collected by peers are base for taking decisions which prevents unauthorized file downloads. Vector based trust metric is based on both interaction and recommendations. If there are sufficient neighbors then reputation query is sent to neighbor otherwise it gets flooded to the network. Separate service and recommendation contexts enabled to compute trustworthiness in large variety of attack scenarios. To model various trusting conditions, a lattice structure with trust and knowledge axis is considered.

3. PROPOSED SYSTEM

In proposed system we use the reccomendation metric, service trust metric to decide the trustworthiness of peers. Fig 1 shows architecture of Peer2Peer environment. Assume that Peer1 wants to access the particular service.Peer3 is a stranger to peer1 (because at beginning each peer is stranger to each other) and a service provider. Peer1 sends recommendation request from its acquaintances (P2 is said to be acquaintance of P1,if P1 had at least one interaction with P2 otherwise it is said to be stranger). Suppose that peer2 sends a back recommendation to peer1. Peer 1 collects all the recommendations from peers and computes reputation value r.

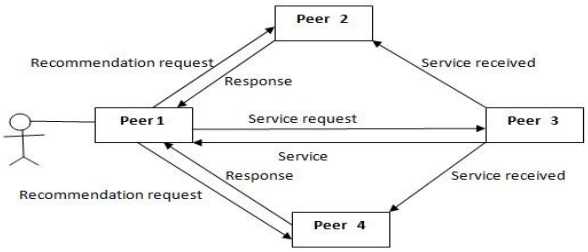

Fig. 1 Architecture of Peer2Peer System

After this, peer1 computes peer2's recommendation and stores result, and updates recommendation trust about peer2.Considering peer3 is trustworthy enough ,peer1 gets service from peer3. Then peer1 evaluates this interaction and computes quality of service and assigns a satisfaction value for interaction. Old interaction's importance decreases as new interaction happens. The fading effect parameter notes this issue and forces peer to stay consistent in the future interactions.

3.1 Service Trust Metric (ST)

In order to evaluate trustworthiness of an aquaintance in the service context, there are two integrants named competence belief and integrity belief values needs to evaluate using the information in its service history. Competence belief explors an aquaintance's satisfaction about past interactions.

Let Cij denotes the competence belief of Pi about Pj in the service context.Competence belief is nothing but the average behavior in the past interaction.Weights and recentness of interactions should be considered in order to evaluate competence. Competence belief Cij can be calculated as follows,

$$Cij = \frac{1}{B} \sum(Sij.Wij.Fij)$$

Where B= (Wij.Fij) is normalization coefficient.Sij=1 if Pj completes all interactions perfectly Cij always takes a valuebetween 0 and 1 because 0<=Sij, Wij, Fij<=1 by defination.

Integrity belief is level of confidence in prediction of future interaction.More prdictable behavior of Pj in future interactions. integrity can be ensured with small value of integrity belief. Then Pi compute STij as follows,

$$STij = Cij - IBij/2$$

3.2 Reputation Metric(Rij)

Trustworthiness of stranger recommendation based is the unit of reputation metric.Suppose P2 is stranger to P1 while P3 is aquaintance of P1,then if P1wanted to compute Rij value, it sends reputation query to collect recommendation from its aquintances.P1 evaluates Rij upon collecting all

recommendations.

Let Ti={P1,P2,……..Pt}is set of peers who holds trustworthiness, and t is number of peers in set A.if Pk had at least one transaction with Pj then it responded as,

- Ckj, IBkj. These are Pk's inteaction histiry with Pj summary
- SHkj.History size with Pj.
- Rij.reputaton values upon arrival of request.
- Nkj.number of aquaintance of Pk.

3.3 Recommendation Trust Metric(RT)

Once reputation metric is computed,based on accuracy of their recommendations peer updtes recommendation trust values of recommenders.Suppose Pi wants particular service,Pj is stanger to Pi as well as service provider.Pi sends request for recommendation from its aquaintance to knowPj's reputation.In response Pk sends recommendation to Pi,upon collecting all recommendation ,Pi computes reputation value.After this,recommendation of Pk is evaluated by peer Pi and updates the recommendation trust metric,then Pi gets service from Pj with consideration of its trustworthy.Once it got service Pi performs evaluation of interactions and updates the value of service trust metric.

3.4 Selection of Service Provider

Service trust metric,service history size,competence belief,and integritybelief values are prime ingrediants for selection of service provider.Suppose when Pi wants to access service like file downloading,it chooses the service provider who have highest service trust value.If condition of service trust value equallity arises then factor of service history size is considered,one who have largest service history size will be get selected as service provider.Stranger can be selected by Pi if it has high reputation.for example Ps is stranger,Pi (who wants to access service) sets service trust metric(STis)=reputation value(Ris).Ps is get selected as a service provider by Pi if trustworthinees of it is more.Reuester can get service from other service provider if provider reaches to its maximum value.This property is used as load balancing mechanism.

Process Sumary

- First user registration will happen and then user can login.
- Then we can take recommend from another peer.
- Calculate the recommendation value.
- Based on this recommendation value we determine that peer is valid or not.
- Then we can determine whether you can take service from that peer or not

4. CONCLUSION AND FUTURE WORK

We have presented trusted model for peer to peer networks. Peer develops trust relationship with peers. Ultimately it can isolate peers who have malicious intents. Service context and recommendation context are two prime contexts which are defined to quantify peer's capabilities in order to provide services and giving recommendations. Fading effect, satisfaction, weight are the parameters to be considered about interaction and recommendations. We can calculate number of trust recommendation given by peer as well as services taken by peer. Based on this, attacker modules calculate the attacks and give feedback about peer. In future we will reduce the storage overhead used to keep trust information.

5. REFERENCES

[1] K.Abererand Z. Despotovic,"Managing Trust in a Peer-2-Peer Information System," Proc. 10th Int'l Conf. Information and Knowledge 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.

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

[6] S. Marsh, "Formalising Trust as a Computational Concept," PhD thesis, Dept. of Math. and Computer Science, Univ. of Stirling,1994.

[7] A. Abdul-Rahman and S. Hailes, "Supporting Trust in Virtual Communities," Proc. 33rd Hawaii Int'l Conf. System Sciences (HICSS), 2000.

[8] B. Yu and M. Singh, "A Social Mechanism of Reputation Management in Electronic Communities," Proc. Cooperative Information Agents (CIA), 2000.

[9] L.Mui, M. Mohtashemi, and A. Halberstadt, "A Computational Model of Trust and Reputation for E-Businesses," Proc. 35th Hawaii Int'l Conf. System Sciences (HICSS), 2002.

[10] A.Jøsang, E. Gray, and M. Kinateder, "Analysing Topologies of Transitive Trust," Proc.First Int'l Workshop Formal Aspects in Security and Trust (FAST), 2003.

[11] S.Song, K. Hwang, R. Zhou, and Y.-K. Kwok, "Trusted P2P Transactions with Fuzzy Reputation Aggregation," IEEE Internet Computing, vol. 9, no. 6, pp. 24-34, Nov.-Dec. 2005.

[12] M.Virendra, M. Jadliwala, M. Chandrasekaran, and S. Upadhyaya, "Quantifying Trust in Mobile Ad-Hoc Networks," Proc. IEEE Int'l Conf. Integration of Knowledge Intensive Multi-Agent Systems (KIMAS), 2005.

[13] Z.Despotovic and K. Aberer, "Trust-Aware Delivery of Composite Goods," Proc.First Int'l Conf. Agents and Peer-to-Peer Computing, 2002.

[14] A.Jøsang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," Decision Support Systems, vol. 43, no. 2, pp. 618-644, 2007.