Towards securing the multiagents using a MOTSOR Model of Trust Self-Organizing Peer-To-Peer System

Baseem Adnan AL-Twajre[1]
University of Babylon - Iraq
altwajresam@gmail.com

Abstract: *Open nature of peer-to-peer system exposes them to malicious activity. Be used to build trust between peers, reducing the attack of malicious peers can. In this paper, we present the distributed algorithm that enables the peer in order to reason about the reliability of other peers based on the recommendation and interaction in the past. By using the available local information, in the vicinity, you can create a trusted network of their own, peer Please do not try to learn the trust global information. Context of two trust recommendation context, service, and are defined to measure the reliability that provides a service and provide recommendations. Recommendations and dialogue, importance, newness, and will be evaluated based on the satisfaction parameters of the peer. In addition, while evaluating the recommendations, trust and confidence of the recommender for recommendation has been considered. The proposed model is able to reduce the attack on the malicious behavior models of 16 different simulation experiments show the file sharing application. In the experiments, good peers, was able to form a trust relationship in the vicinity, to isolate malicious peers.*

Index Terms: *Peer-to-peer systems, trust management, reputation, and security.*

1. INTRODUCTION

In order to accomplish the task, peer-to-peer (P2P) systems rely on the cooperation of the peers. Ease is a threat to the security of the P2P system may perform malicious activities. When you create a trust long-term relationships between peers, by reducing the risks and uncertainties in the interaction of P2P in the future, you will be able to provide a more secure environment. However, establishing a trust entity unknown, it is difficult for malicious environment. In addition, be measured in a numerical concept and social, it is difficult to trust. Metric is required to represent the reliability of the calculation model. Is not enough in most cases to classify the peers as either reliable, or of unreliable. It is possible that peer to rank according to reliability, you must have the accuracy of the metric. Peer feedback and interaction, provides information for determining the trust between the peers. Interaction with peers, provides certain information about the peer, but there are cases where false information is included feedback. Evaluation of reliability will be an issue this.

In the presence of authority, for example, the central server, is the preferred way to store and manage credit information, and eBay. Safely, store the trust information, the central server, to define the trust metric. The P2P system most, because there is no central server, to organize themselves in order to store and manage the trust information about each other peer, [1], [2]. Trust management information is dependent on the structure of the P2P network. The approach of the distributed hash table (DHT) based, by each peer stores a feedback about other peers will trust holder [1], [3], [4]. You can then be accessed via the DHT efficient global trust information that contains the trust holders. In networks that are not structured, each peer may interact storing past trust information about the peer or peers in the vicinity of [2], [5], and [6]. In order to learn the trust information for other peers, peer sends a query trust. Trust query will be sent to the vicinity of the query initiator or flooding in both networks. In general, it is not global, credit information calculated and does not reflect the opinions of all peers.

By establishing a trust relationship between peers close propose self-organization trust model that aims to reduce malicious activity in P2P system. No, it has not been used for trusted peer or prior information to leverage the establishment of a trust relationship. Peer Please do not try to collect the trust information from all peers. Each peer, has developed a local view of its own trust on peer interaction in the past. In this way, peer excellent, which can form a dynamic trust groups in the vicinity, to separate the malicious peer. Since there is a tendency for peer to form a trust relationship in close proximity to the peer in general, to interact with the small set peer [7], and helps to reduce the attack of a P2P system.

In MOTSOR, in the beginning, the peer is considered a stranger to each other. Etc. to upload a file, the peer will be the acquaintance of another peer after providing the service. If there is no acquaintance at all peers, it will choose to trust a stranger. Acquaintance is more preferable than others whenever you can trust in the same way as they. Using the services of the peer, it is the interaction that freshness of the interaction with the weights (importance), and are evaluated on the basis of the satisfaction of the requestor. Feedback of peer acquaintance, about the recommendation, will be evaluated based on the reliability of the recommender. It, the level of confidence of the recommendation has been included experience of recommender own collection peer, and information, the recommendation from a friend of the recommender. If the reliability is low, has a value evaluation is low, recommended, affects the reliability of the following recommendations.

Peers, is a provider of good service and vice versa, may be recommended or bad. The thinking in this way, and give a variety of tasks such as recommendation to provide a MOTSOR service, which defines the context of two of the trust. The service recommendation context. In the context of the following information about the recommendations and the interaction of the past, are stored in the history of the individual in order to evaluate the integrity and ability of acquaintance.

It will define a trust metric of one MOTSOR3. Reputation metric is calculated based on the recommendation. It is important in deciding about a new acquaintance with a stranger. Experience as acquaintance with the increases, the reputation to lose its importance. Recommendation trust and trust services is the primary metric for measuring the reliability in the context of and recommendations for each service. When selecting a service provider, reliability metrics of the service is used. Recommendation trust metric is important when requesting a recommendation. When calculating the reputation metrics recommendations are evaluated based on the recommendation trust metric.

We conducted our experiments to attack that implements the P2P file sharing simulation tools, to relax is to understand the impact of MOTSOR. (Number bandwidth, shared file) ability, (online / offline period, waiting for the session) and the behavior of peers, parameters that are related to the peer (the popular file size, file) resource allocation, some it is approximately the same as empirical results of [8], [9], [10]. It was able to make observations more realistic about the evolution of the trust relationship. Run the service of both, we studied, the 16 kinds of peer behavior recommendation- malicious attacks of the base. In the case of MOTSOR all, to reduce the attack of service-based. The malicious peer, for example, unless it is 50% of all peers in a large amount, recommendation based attacks, was included. Peer experiment is good in the MOTSOR program cannot have a credit global information, to protect themselves against malicious peer. Trust metric of MOTSOR is, let's evaluate the reliability of the peer of other peers based on local information. Context and recommendations services, can be measured with good confidence that provides a service and provide recommendations.

2. RELATED WORK

Marsh [11] defines a formal trust model based on sociological foundations. An agent used their own experiences to build relationships of trust and does not take into account information from other agents. Abdul-Rahman and Hailes [12] evaluated the confidence in a discrete domain as an aggregation of experiences and recommendations of other parties directly. Define a semantic distance measure to test the accuracy of the recommendations. Model Yu and Singh [13] trust information is propagated through chains of reference. The references are the primary method of developing trust in others. Mui et al. [14] propose a statistical model based on trust, reputation, and the concepts of reciprocity. The reputation spreads across multiple reference strings. Josang et al. [15] argue that the references indirect relationships based on trust can cause incorrect derivation of confidence. Therefore, the topologies of trust must be carefully evaluated before the spread of reliable information. Terzi et al. [16] introduce an algorithm to classify users and assign roles based on trust. Zhong [17] proposes a concept of dynamic trust model based on social trust McKnight [18]. When building trust relationships, uncertain evidence is evaluated using probability and second order under Dempster-Shaferian.

In the e-commerce platforms, reputation systems are widely used as a method of building trust, for example, eBay, Amazon and Epinions. A central authority collects testimonials from previous clients, which are used by customers in future purchasing decisions. Resnick et al. [19] discusses the relationships that ensure long life, forcing assessments, check the honesty of the recommendations are some difficulties in reputation systems. Despotovic and Aberer [20] point out that the exchange of confidence-aware can increase economic activity, as some exchanges cannot happen without trust. Jsang et al. [21] indicate that reputation systems are vulnerable to attacks from incorrect and false feedback. So vote totals should be based on objective criteria to be useful. Dellarocas [22] proposes methods for controlled anonymity and cluster filtering as countermeasures to unfairly high / low ratings and discriminatory attacks seller behavior. Yu and Singh [23] present an algorithm for weighted majority against three attacks on reputation: complementary, exaggerated positive / negative evaluations. Guha et al. [24] use concepts of trust and distrust in a discrete domain. His results in the website Epinions data show that distrust is useful for measuring the reliability accurately. Reputation systems are vulnerable to Sybil attacks [25], in which a malicious entity can spread false assessments, creating several false entities. To defend against Sybil attacks Yu et al. [26] and Tran et al. [27] propose solutions based on the observation that many false entities generally have trust relationships with each other techniques, but rarely have relationships with real users.

Models of trust in P2P systems have additional challenges compared to e-commerce platforms.

Malicious peers are more likely to attack P2P trust models due to the lack of a central authority. Hoffman et al. [28] discuss five common attacks in P2P trust models: white wash aggrandizement, slander, orchestrated, and denial of service attacks. Said the defense techniques in trust models depend on the architecture of P2P system. In a structured P2P system, DHT structure can provide decentralized and efficient access to trust information. In Aberer and Despotovic trust model [1], peers report their complaints by using P-Grid [29]. A peer is assumed to be reliable unless there are complaints about it. However, the pre-existence of trust between partners does not distinguish a newcomer and one unreliable. Eigen trust [3] uses the transitivity of trust to calculate the global trust values stored in CAN [30]. Trusted companions used to take advantage of building trust between regular peers and mitigate some attacks collaboration. Peer Trust [4] defines the transaction parameters and context of the community for the adaptive computation confidence in P-Grid. While transaction context parameter addresses the application dependent factors, addresses community issues community context of P2P related parameters, such as creating incentives to force evaluations. Both Peer trust and Eigen trust and evaluate a recommendation based on the trustworthiness of the recommender. Song et al. [31] propose a trust model based on fuzzy-logic in line [32], which performs similar results Eigen trust least loaded message. Power Trust [33] builds an overlay network based on the law of energy distribution of peer reviews. By using a strategy of random walk and using power nodes, aggregation rate feedback and global reputation accuracy are improved. A structured network solutions are based on a structure of DHT to store trust information. Each pair becomes a trusted support another partner, which is supposed to provide authentic information of confidence. However, the holder of the trust may be malicious and provide inauthentic information. In MOTSOR, rather than considering feedback from a holder of personal trust in the authentic, the public opinion of all known is seen as a more credible information. Instead of considering the information of global confidence, trust information locally is enough to make decisions as partners to develop their own networks of trust.

In unstructured P2P systems, background queries are generally flooded to the entire network. Cornelli et al. [34] queries confidence flooding in the Gnutella [9] network. A detailed computational model of trust is not defined. Peers make decisions based on assessments collected to mitigate downloads inauthentic files. Selcuk et al. [5] present a metric vector-based trust trusting both interactions and recommendations. A reputation query is sent to the neighbors if enough neighbors. Otherwise, the query is flooded to the network. Although five types of malicious peers, based on the recommendation attacks were studied are not considered in the experiments. Yu et al. [35] store a history of interactions and consider the qualifications and recency of interactions in evaluating trust. Number of interactions with a partner is a measure of confidence in the peer. GossipTrust [6] defines a randomized gossip protocol [36] for efficient aggregation of trust values. A query is randomly referred to some neighbors instead of all neighbors. Compared to the approach flooding reduces gossip reputation query traffic. In MOTSOR, peers send queries only to peers reputation interacted in the past, which reduces network traffic in comparison to the flooding based approaches. Furthermore, each extends his companions trusted network over time and can get more credible recommendations known.

Some trust models signed credentials used to store information in confidence. Ooi et al. [37] propose that each peer stores its own reputation by signed certificates. When a teammate needs to know about a stranger asks foreign certificates. NICE [38] uses cookies signed as evidence of good conduct. Peers trust dynamically formed groups to protect each other. Peers in the same group are more confident. Pricing based on trust and trade policies help protect the integrity of the groups. The use of signed credentials eliminates the need for reputation queries, but ensuring the validity of the trust information in the credentials is a problem. If a partner misbehaves after picking good credentials, it is difficult to revoke credentials without using a central authority. Moreover, generally a public key infrastructure is needed. How to evaluate the interactions and how to define trust metrics are important problems in trust models. Wang and Vassileva [39] propose a Bayesian network model that uses different aspects of interactions in an application of P2P file sharing. Victor et al. [40] define metric trust and distrust. A nonzero value distrust allows an agent to distinguish an untrusted user to a new user. A network structure with axis confidence and knowledge is used to model various conditions of trust. Swamynathan et al. [41] decouple trust metrics in the context of service evaluating and recommending the best reliability. Creating contexts of trust can be useful to address issues in various fields. Gupta et al. [42] use reputation as a coin. A central agent issues money to his colleagues in return for their services to others. This money can be used to obtain a better quality of service. Bhargava et al. [43] discusses privacy negotiation to gain more confidence in pervasive systems. In another interesting study, Virendra et al. [44] use trust concept in mobile ad-hoc networks to establish keys between nodes and cluster nodes into domains. Reliability is measured according to the lost and misdirected packages. Phases of confidence-defined for the implementation of new nodes, maintaining the confidence of their age mates, and restoring confidence in the malicious nodes.

In MOTSOR, to evaluate the interactions and recommendations better, importance, recent, and satisfaction parameters are considered peers. Honesty and trust recommendation on Recommender considered in evaluating the recommendations. In addition, service contexts and recommendation are separated. This allowed us to measure the reliability in a variety of attack scenarios. Most trust models fail to consider how interactions are valued and assume that there is a rating system. In this study, a rating system interaction in a file sharing application and consider many parameters in real life to make more realistic simulations suggested.

3. MOTSOR Model Description

3.1 Introduction of trust model

Trust is a degree of belief. Based on the principles of trust, trust model is created. In this design, several colleagues connect and interact with each other for file sharing and downloading. Once all peers are connected to the database, one partner is chosen for interaction. Reliability of a torque is calculated based on service metrics, recommendation and reputation. After each interaction known list is updated. The service trust metric is calculated based on the bandwidth and transaction time. Also the confidence value of each pair is calculated by fading effect, competition and the belief of integrity. With these calculated values of trust, reputation and recommendation metric metrics are evaluated by file parameters importance, regency and satisfaction. All companions are assumed to be strange at first. Peers must help others in order to build trust. A trusted partner cannot observe all the interactions in a P2P system, and could be a source of misleading information. A peer becomes an acquaintance of another partner after providing a service to it. Using a service is called a partner service interaction. A recommendation represents data from a known confidence about a stranger. A requesting peer recommendations only acquaintances. No reliable partners to manage trust relationships. Some colleagues behave evil but some may behave confidence. Peers periodically stop and join the network.

3.2 Interaction Process

The interaction process takes place by connecting all the peers that wish to upload and download the files in which peers are denoted by p, for example i^{th} peer can be represented as pi. The Interaction process consists of two phases.

a) Upload process
b) Download process

When pi uses a service of p_j, a service interaction for pi occurs. Unidirectional of interaction occurs. p_j is stranger to pi, if pi has no service interaction with p_j . p_i set of acquaintances is denoted by Ai .Each peer stores a transaction history of service interactions for each acquaintance. pi‘s service history with pj is denoted as SH_{ij}.. SH_{ij} is a time ordered list, since new interactions are appended to the history. After finishing a service interaction, pi evaluates quality of the service. $0\leq ek_{ij} \leq 1$ denotes p_i satisfaction about k^{th} service interaction with pj. If the interaction is cancelled, ek_{ij} gets 0 value. K is the sequence number of the interaction in SH_{ij} . A service interaction is associated with a weight to quantify importance of the interaction. $0 \leq wk_{ij} \leq 1$ denotes the weight of k^{th} service interaction of pi with p_j.

In upload process, all the peers can upload their files to share with other peers, and it is designed by peers origin and terminal. The file is shared by allocating it to other concerned peer. Once the file is shared, acquaintance list is updated in order to know its neighborhood process that has interacted. In upload process, the quality of service is calculated. The quality of service is calculated based on bandwidth, transaction time. In download process, the recommendation and reputation of peers are evaluated.

3.3 Service Trust metric (st_{ij})

A peer becomes an acquaintance of another peer after providing a service. Using a service from a peer is called a service interaction. Trustworthiness of a service provider is based on the trustworthiness of its services and rates of its properties. In addition to providers‟ properties, a provider can provide important clues for requestors to assess its trustworthiness. The importance of an interaction fades as new interactions happen. $0\leq f\,k_{ij} \leq 1$ denotes the fading effect of k^{th} service interaction of pi with pj. It is calculated as follows:

$$f_{ij}^{k} = \frac{K}{sh_{ij}} \; ; 1 \leq k \leq sh_{ij}$$

A peer first calculates competence and integrity belief values using the information about service interactions. Competence belief is based on how well an acquaintance satisfies the needs of interactions. cb_{ij} denotes the competence belief of pi about pj in the service context. Competence belief is measured based on average behavior in the past interactions. The cb_{ij} is calculated as follows:

$$cb_{ij} = \frac{1}{\beta cb}\sum_{k=1}^{sh_{ij}}(s_{ij}^{k} \cdot w_{ij}^{k} \cdot f_{ij}^{k})$$

$\beta cb = \sum_{k=1}^{sh_{ij}}(w_{ij}^{k}.f_{ij}^{k})$Is the normalization coefficient.

The confidence level about the prediction of future interactions is called integrity belief. ib_{ij} denotes the integrity belief of pi about p_j in the service context. The measure of integrity belief is the deviation from the average behavior. Therefore, ib_{ij} is calculated as:

$$ib_{ij} = \sqrt{\frac{1}{sh_{ij}}\sum_{k=1}^{sh_{ij}}(s_{ij}^{k}.w_{ij}^{\mu}.f_{ij}^{\mu} - cb_{ij})^2}$$

If pi sets st_{ij} = cb_{ij} , half of the future interactions will likely to have a satisfaction value less than cb_{ij} . Thus, st_{ij} = cb_{ij} is an over-estimate for p_js trustworthiness. A lower estimate makes pi more confident about future decisions with p_j . p_i may calculate stij as follows:

$$st_{ij} = cb_{ij} - ib_{ij}/2$$

3.4 Reputation Trust Metric (r_{ij})

Reputation metric is a trusted agent who keeps track of the behavior of other agents. Assume that pj is an intruder to p_i; if pi needs a service from p_j,it sends a recommendation request to nearby peer p_k . p_i selects trustworthy acquaintances and a threshold is set. After collecting all recommendations, p_i calculates er_{ij}, an estimation for the reputation of p_j, by aggregating r_{kj} values in the recommendations. r_{kj} should be considered with respect to η_{kj}.

$$er_{ij} = \frac{1}{\beta er}\sum_{p_k \in T_i}(rt_{ik}.\eta_{kj}.r_{kj})$$

Then, p_i calculates estimations for the competence and integrity beliefs about pj which are denoted by ecb_{ij} and eib_{ij} respectively. These values are calculated by aggregating cb_{kj} and ib_{kj} values in the recommendations. cb_{kj} and ib_{kj} should be evaluated based on sh_{kj}.

$$r_{ij} = \frac{\lfloor \mu_{sh} \rfloor}{sh_{max}}(ecb_{ij} - eib_{ij}/2) + \left(1 - \frac{\lfloor \mu_{sh} \rfloor}{sh_{max}}\right) er_{ij}$$

3.5 Recommendation Trust Metric (rt_{ik})

The trust-based recommendation approach, which provides recommendations to a requester in a trust network, is built on a vertex similarity measurement between graphs. After calculating r_{ij} value, p_i updates recommendation trust values of recommenders also pi updates rt_{ik}, according to peer recommendation. p_i compares competency , integrity, reputation values of p_i and pj with p_k and p_j . If these values are close, then p_k recommendation is good and a high trust value is assigned.

$$rt_{ik} = \frac{rh_{ik}}{rh_{max}}(rcb_{ik} - rib_{ik}/2) + \frac{rh_{max} - rh_{ik}}{rh_{max}} r_{ik}$$

3.6 Trust value evaluation

The trust evaluation is done based on the three metrics that measures quality of service, opinion values and suggestions. The trust value of all the peers are evaluated and validated. Thus the graph is plotted based on trust values of the three peers and the peer with highest trust value is displayed and chosen as the best service provider.

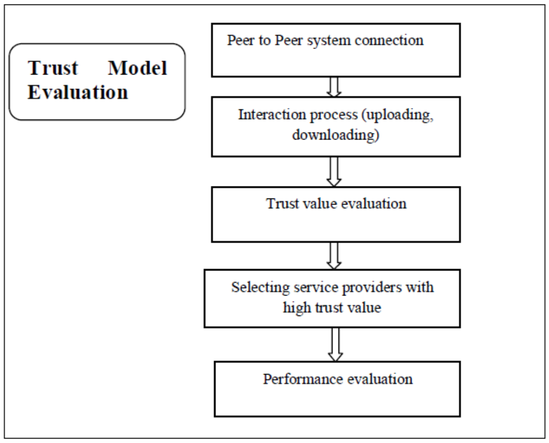
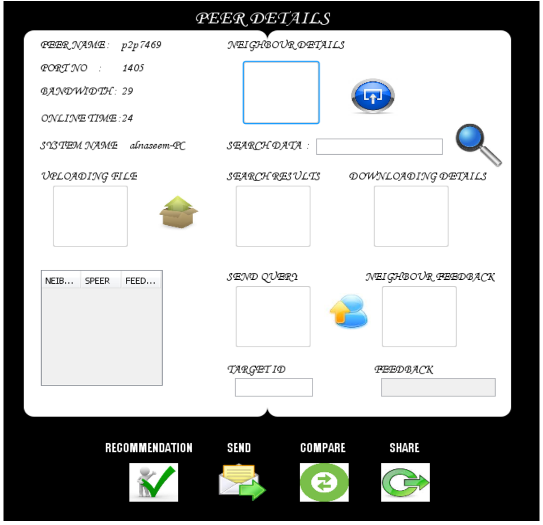

Trust Model Evaluation
Peer to Peer system connection
Interaction process (uploading, downloading)
Trust value evaluation
Selecting service providers with high trust value
Performance evaluation

Figure 1: Architecture Flow of the Process

4. RESULTS

To evaluate this approach, we implemented a simulation using .NET framework and its tools. The figure2 give a description about the peer details.



PEER DETAILS

PEER NAME : p2p7469

PORT NO : 1405

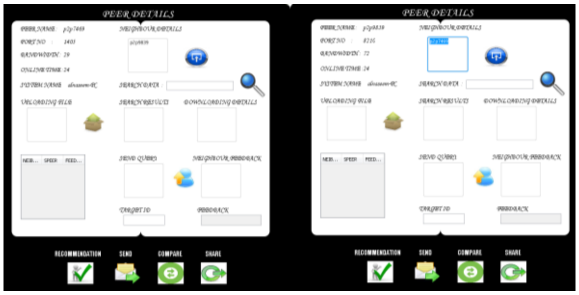
BANDWIDTH : 29

ONLINE TIME : 24

SYSTEM NAME alnaseem-PC

Figure 2: Peer Details

The theme of the concept, the peer-peer services will exchange the data (sharing the information between the end-end users) will observer on the following figure3.



PEER DETAILS

PEER NAME : p2p7469
PORT NO : 1403
BANDWIDTH : 29
ONLINE TIME : 24
SYSTEM NAME

PEER DETAILS

PEER NAME : p2p9839
PORT NO : 8216
BANDWIDTH : 72
ONLINE TIME : 24
SYSTEM NAME

Figure 3: Peer-Peer Exchanging Data

To sharing the data between peer-peer will find the multiple user information like port no, peer name and data needs to request the end user. The end user is valid or not will decide by the MoTSOR, to evaluate the time taken to this approach its representing as the Recommendation Request process time. The time taken by each recommendation request process of difference peer user with the effect of data sharing in figure 4.

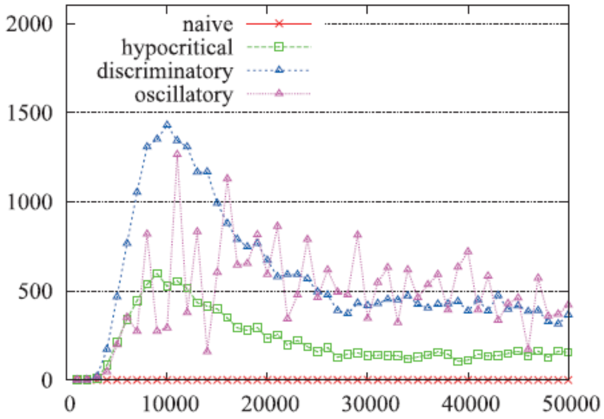


Figure 4: Recommendation Request Time

5. CONCLUSION

The peer, it is possible to develop a trusted network in the vicinity, trust model for P2P networks is presented. To develop a relationship of trust with good fellow, it peers, will be able to separate the malicious peer around itself. Two trusted context, the recommendation service context is defined to measure the ability of the peer that provides the service, to provide recommendations. And recommendations dialogue is considered satisfaction, weight, and the fading effect parameters. Recommendation contains the level of trust of the recommendations of the recommendation experience themselves, and information, from the acquaintance. These parameters, gave a better evaluation of the reliability to us.

Personal, collaboration, and change pen name, an attacker, has been studied in the experiment. Damage pseudospoofing and collaboration is dependent on the behavior of the attack. Recommendation is important in cooperation attacks and vibration hypocrisy, and pseudospoofers, but, discriminatory and naive, the attacker is very useful to them. To reduce both the attack of the recommendations based in most experiments services and MOTSOR. However, in a very vicious environment as a network malicious such as 50% that co-workers will be able to continue to disseminate large amounts of recommendation misleading. Another problem for the MOTSOR is to maintain the confidence on all networks. If you change the point of attachment to the network, you may lose some of the trust network it peer. These problems might be studied as future work to extend the trust model.

With the trust information, it does not solve the security problem of all P2P system, it is possible to enhance the safety and efficacy of the system. If the interaction is modeled correctly, it can be shared P2P applications such various MOTSOR, the CPU, storage network, and adapt the P2P game. Be used to define the context of application-specific metrics associated with trust, will help you to evaluate the reliability for a variety of tasks.

References

1. K. Aberer and Z. Despotovic, “Managing Trust in a Peer-2-Peer Information System,”2001.
2. F. Cornelli, E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Samarati, “Choosing Reputable Servents in a P2P Network”, 2002.
3. S. Kamvar, M. Schlosser, and H. Garcia-Molina, “The (Eigentrust) Algorithm for Reputation Management in P2P Networks”, 2003.
4. L. Xiong and L. Liu, “Peertrust: Supporting Reputation-Based Trust for Peer-to-Peer Ecommerce Communities,”July 2004.
5. A.A. Selcuk, E. Uzun, and M.R. Pariente, “A Reputation-Based Trust Management System for P2P Networks”, 2004.
6. R. Zhou, K. Hwang, and M. Cai, “Gossiptrust for Fast Reputation Aggregation in Peer-to-Peer Networks,” Sept. 2008.
7. J. Kleinberg, “The Small-World Phenomenon: An Algorithmic Perspective,” 2000.
8. S. Saroiu, P. Gummadi, and S. Gribble, “A Measurement Study of Peer-to-Peer File Sharing Systems,” 2002.
9. M. Ripeanu, I. Foster, and A. Iamnitchi, “Mapping the Gnutella Network: Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design,” Jan. 2002.
10. S. Saroiu, K. Gummadi, R. Dunn, S.D. Gribble, and H.M. Levy, “An Analysis of Internet Content Delivery Systems,” 2002.
11. S. Marsh, “Formalising Trust as a Computational Concept,”1994.
12. A. Abdul-Rahman and S. Hailes, “Supporting Trust in Virtual Communities,” 2000.

13. B. Yu and M. Singh, “A Social Mechanism of Reputation Management in Electronic Communities,” 2000.
14. L. Mui, M. Mohtashemi, and A. Halberstadt, “A Computational Model of Trust and Reputation for E-Businesses,” 2002.
15. A. Jøsang, E. Gray, and M. Kinateder, “Analysing Topologies of Transitive Trust,” 2003.
16. E. Terzi, Y. Zhong, B. Bhargava, Pankaj, and S. Madria, “An Algorithm for Building User-Role Profiles in a Trust Environment,” 2002.
17. Y. Zhong, “Formalization of Dynamic Trust and Uncertain Evidence for User Authorization,” 2004.
18. D.H. McKnight, “Conceptualizing Trust: A Typology and E-Commerce Customer Relationships Model,” 2001.
19. P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, “Reputation Systems,” 2000.
20. Z. Despotovic and K. Aberer, “Trust-Aware Delivery of Composite Goods,” 2002.
21. A. Jøsang, R. Ismail, and C. Boyd, “A Survey of Trust and Reputation Systems for Online Service Provision,” 2007.
22. C. Dellarocas, “Immunizing Online Reputation Reporting Systems Against Unfair Ratings and Discriminatory Behavior,” 2000.
23. B. Yu and M.P. Singh, “Detecting Deception in Reputation Management,” 2003.
24. R. Guha, R. Kumar, P. Raghavan, and A. Tomkins, “Propagation of Trust and Distrust,” 2004.
25. J. Douceur, “The Sybil Attack,” 2002.
26. H. Yu, M. Kaminsky, P.B. Gibbons, and A. Flaxman, “Sybilguard: Defending against Sybil Attacks via Social Networks,” 2006.
27. N. Tran, B. Min, J. Li, and L. Subramanian, “Sybil-Resilient Online Content Voting,” 2009.
28. K. Hoffman, D. Zage, and C. Nita-Rotaru, “A Survey of Attack and Defense Techniques for Reputation Systems,” 2009.
29. K. Aberer, A. Datta, and M. Hauswirth, “P-Grid: Dynamics of Self- Organization Processes in Structured P2P Systems,” 2005.
30. S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker, “A Scalable Content-Addressable Network,” 2001.
31. S. Song, K. Hwang, R. Zhou, and Y.-K. Kwok, “Trusted P2P Transactions with Fuzzy Reputation Aggregation,” 2005.
32. I. Stoica, R. Morris, D. Karger, M.F. Kaashoek, and H. Balakrishnan, “Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications,” 2001.
33. R. Zhou and K. Hwang, “Powertrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing,” Apr. 2007.
34. F. Cornelli, E. Damiani, S.D.C. di Vimercati, S. Paraboschi, and P. Samarati, “Implementing a Reputation-Aware Gnutella Servent,” 2002.
35. B. Yu, M.P. Singh, and K. Sycara, “Developing Trust in Large- Scale Peer-to-Peer Systems,” 2004.
36. S. Boyd, A. Ghosh, B. Prabhakar, and D. Shah, “Randomized Gossip Algorithms,” June 2006.
37. B. Ooi, C. Liau, and K. Tan, “Managing Trust in Peer-to-Peer Systems Using Reputation-Based Techniques,” 2003.
38. R. Sherwood, S. Lee, and B. Bhattacharjee, “Cooperative Peer Groups in Nice,” 2006.
39. Y. Wang and J. Vassileva, “Bayesian Network Trust Model in Peer-to-Peer Networks,” 2003.
40. P. Victor, C. Cornelis, M. De Cock, and P. Pinheiro da Silva, “Gradual Trust and Distrust in Recommender Systems,” 2009.
41. G. Swamynathan, B.Y. Zhao, and K.C. Almeroth, “Decoupling Service and Feedback Trust in a Peer-to-Peer Reputation System,” 2005.
42. M. Gupta, P. Judge, and M. Ammar, “A Reputation System for Peer-to-Peer Networks,” 2003.
43. S. Staab, B. Bhargava, L. Lilien, A. Rosenthal, M. Winslett, M. Sloman, T. Dillon, E. Chang, F.K. Hussain, W. Nejdl, D. Olmedilla, and V. Kashyap, “The Pudding of Trust,” 2004.
44. M. Virendra, M. Jadliwala, M. Chandrasekaran, and S. Upadhyaya, “Quantifying Trust in Mobile Ad-Hoc Networks,” 2005.
45. E.J. Friedman and P. Resnick, “The Social Cost of Cheap Pseudonyms,” J. Economics and Management Strategy, vol. 10, no. 2, pp. 173-199, 2001.
46. S. Xiao and I. Benbasat, “The Formation of Trust and Distrust in Recommendation Agents in Repeated Interactions: A Process- Tracing Analysis,” 2003.
47. A. Habib, D. Xu, M. Atallah, B. Bhargava, and J. Chuang, “A Tree- Based Forward Digest Protocol to Verify Data Integrity in Distributed Media Streaming,” July 2005.