International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

Services Based On Trustworthiness in P2p Networks

Swetha Reddy Kalam
Telangana Social Welfare Degree College For Women

ABSTRACT

Open nature of 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. Peers create their own trust network in their proximity by using local information available and do not try to learn global trust information. Two contexts of trust, service, and recommendation contexts are defined to measure trustworthiness in providing services and giving recommendations. Interactions and recommendations are evaluated based on importance, recentness, and peer satisfaction parameters. Additionally, recommender's trustworthiness and confidence about a recommendation are considered while evaluating recommendations. Simulation experiments on a file sharing application show that the proposed model can mitigate attacks on 16 different malicious behavior models. In the experiments, good peers were able to form trust relationships in their proximity and isolate malicious peers.

Keywords : peer to peer, malicious behavior models, isolate malicious peers

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.

However, establishing trust in an unknown entity is difficult in such a malicious environment. 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 trustworthiness a challenge. In the presence of an authority, a central server is a preferred way to store and manage trust information, e.g., eBay. The central server securely stores trust information and defines trust metrics. Since there is no central server in most P2P systems, peers organize themselves to store and manage trust information about each other .

A file sharing simulation program is implemented in Java tool serve results of using SORT in a P2P environment. Some Questions studied in the experiments are as follows: how SORT handles attacks, how much attacks can be mitigated, how much recommendations are (not) helpful in correctly identifying malicious peers, and what type of attackers are the most harmful No trust. Trust information is not used for uploader selection. An uploader is selected according to its bandwidth. T his method is the base case to understand if trust is helpful to mitigate attacks.. No reputation query. An uploader is selected based on trust information but peers do not request recommendations from other peers. Trust calculation is done based on SORT equations but reputation(r) value is always zero for a peer. This method will help us to assess if recommendations are helpful

1.2 PROBLEM DEFINITION

Management of trust information is dependent to the structure of P2P network. In distributed hash table (DHT)- based approaches, each peer becomes a trust holder by storing feedbacks about other peers . Global trust information stored by trust holders can be accessed through DHT efficiently. In unstructured networks, each peer stores trust information about peers in its neighborhood or peers interacted in the past . A peer sends trust queries to learn trust information of other peers. A trust query is either flooded to the network or sent to neighborhood of the query initiator. Generally, calculated trust information is not global and does not reflect opinions of all peers. We propose a Self-ORganizing Trust model (SORT) that 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. Since peers generally tend to interact with a small set of peers [7], forming trust relations in proximity of peers helps to mitigate attacks in a P2P system. In SORT, peers are assumed to be strangers to each other at the beginning. A peer becomes an acquaintance of another peer after providing a service, e.g., uploading a file. If a peer has no acquaintance, it chooses to trust strangers. An acquaintance is always preferred over a stranger if they are equally trustworthy. Using a service of a peer is an interaction, which is evaluated based on weight (importance) and recentness of the interaction, and satisfaction of the requester. An acquaintance's feedback about a peer, recommendation, is evaluated based on recommender's trustworthiness. It contains the recommender's own experience about the peer, information collected from the recommender's acquaintances, and the recommender's level of confidence in the recommendation. If the level of confidence is low, the recommendation has a low value in evaluation and affects less the trustworthiness of the recommender.

1.3 OBJECTIVE

Open nature of 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. Peers create their own trust network in their proximity by using local information available and do not try to learn global trust information. Two contexts of trust, service, and recommendation contexts are defined to measure trustworthiness in providing services and giving recommendations. Interactions and recommendations are evaluated based on importance, recentness, and peer satisfaction parameters. Additionally, recommender's trustworthiness and confidence about a recommendation are considered while evaluating recommendations. Simulation experiments on a file sharing application show that the proposed model can mitigate attacks on 16 different malicious behavior models. In the experiments, good peers were able to form trust

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

relationships in their proximity and isolate malicious peers.

1.4 ALGORITHM USED

pi denotes the I th peer. When pi uses a service of another peer, it is an interaction for pi. Interactions are unidirectional. For example, if pi downloads a file from pj, it is an interaction for pi and no information is stored on pj.If pi had at least one interaction with pj, pj is an acquaintance of pi. Otherwise, pj is a stranger to pi. Ai denote spi's set of acquaintances. A peer stores a separate history of interactions for each acquaintance. S Hij denotes pi's service history with pj where shij denotes the current size of the history. Sh max denotes the upper bound for service history size. Since new interactions are appended to the history ,SHij is a time ordered list. Parameters of an interaction. After finishing an interaction, pi evaluates quality of service and assigns a satisfaction value for the interaction. Let 0 _ skij _ 1 denote pi's satisfaction about kth interaction with pj. If an interaction is not completed, skij ¼ 0. An interaction's importance is measured with a weight value. Let 0 _ wkij _ 1 denote the weight of kth interaction of pi with pj. Semantics to calculate skij and wkij values depend on the application.

ALGORITHMS USED:

Algorithm 1. GETRECOMMENDATIONS(p_j)

$\mu_{rt} \Leftarrow \frac{1}{|A_i|} \sum_{p_k \in A_i} rt_{ik}$
$\sigma_{rt} \Leftarrow \frac{1}{|A_i|} \sqrt{\sum_{p_k \in A_i} (rt_{ik} - \mu_{rt})^2}$
$th_{high} \Leftarrow 1$
$th_{low} \Leftarrow \mu_{rt} + \sigma_{rt}$
$rset \Leftarrow \emptyset$
while $\mu_{rt} - \sigma_{rt} \leq th_{low}$ and $|rset| < \eta_{max}$ **do**
  for all $p_k \in A_i$ **do**
    if $th_{low} \leq rt_{ik} \leq th_{high}$ **then**
      $rec \Leftarrow$ RequestRecommendation(p_k,p_j)
      $rset \Leftarrow rset \cup \{rec\}$
    end if
  end for
  $th_{high} \Leftarrow th_{low}$
  $th_{low} \Leftarrow th_{low} - \sigma_{rt}/2$
end while
return $rset$

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

Algorithm shows how pi selects trustworthy acquaintances and requests their recommendations. Let _max denote the maximum number of recommendations that can be collected in a reputation query and jSj denote the size of a set S. In the algorithm, pi sets a high threshold for recommendation trust values and requests recommendations from highly trusted acquaintances first. Then, it decreases the threshold and repeats the same operations.To prevent excessive network traffic, the algorithm stopswhen _max recommendations are collected or the threshold drops under minimum value. Based on the past interactions with pj, pi has an expectation about future nteractions. pi wants to maintain a level of satisfaction according to this expectation. If the satisfaction parameter is assumed to follow a normal distribution, cbij and ibij can be considered as approximations of mean and standard deviation of the satisfaction parameter, respectively.

II. EXISTING SYSTEM:

In the existing system of an authority, a central server is a preferred way to store and manage trust information, e.g., eBay. The central server securely stores trust information and defines trust metrics. Since there is no central server in most P2P systems, peers organize themselves to store and manage trust information about each other. Management of trust information is dependent to the structure of P2P network. In distributed hash table (DHT) - based approaches, each peer becomes a trust holder by storing feedbacks about other peers. Global trust information stored by trust holders can be accessed through DHT efficiently. In unstructured networks, each peer stores trust information about peers in its neighborhood or peers interacted in the past. A peer sends trust queries to learn trust information of other peers. A trust query is either flooded to the network or sent to neighborhood of the query initiator.

DISADVANTAGES OF EXISTING SYSTEM

1.Calculated trust information is not global and does not reflect opinions of all peers.

2.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.

3.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

4.Five common attacks in P2P trust models: self-promoting, white-washing, slandering, orchestrated, and denial of service attacks.

III. PROPOSED SYSTEM

In the proposed system, we introduce a Self-Organizing Trust model (SORT) that 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. Since peers generally tend to interact with a small set of peers forming trust relations in proximity of peers helps to mitigate attacks in a P2P system.

ADVANTAGES OF PROPOSED SYSTEM

1.Recommendation-based attacks were contained except when malicious peers are in large numbers, e.g., 50
percent of all peers.

2.Experiments on SORT show that good peers can defend themselves against malicious peers metrics let a peer assess trustworthiness of other peers based on local information.

3.Service and recommendation contexts enable better measurement of trustworthiness in providing services and giving recommendations.

IV. IMPLEMENTATION

1.Peer Creation

2.Upload Process

3.Interaction Process

4.Recommendation

1.PEER CREATION

In this module, we create three peers. In SORT, peers are assumed to be strangers to each other at the beginning. A peer becomes an acquaintance of another peer after providing a service, e.g., uploading a file. If a peer has no acquaintance, it chooses to trust strangers. An acquaintance is always preferred over a stranger if they are equally trustworthy. We implemented a P2P file sharing simulation tool and conducted experiments to understand impact of SORT

2. UPLOAD PROCESS

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

In this module, we design each peer can upload file and its updated to all the peers. The details of each file with their file name, up-loader name with their IP address are stored continuously. So the peer which needs the file can download it.

3. INTERACTION PROCESS

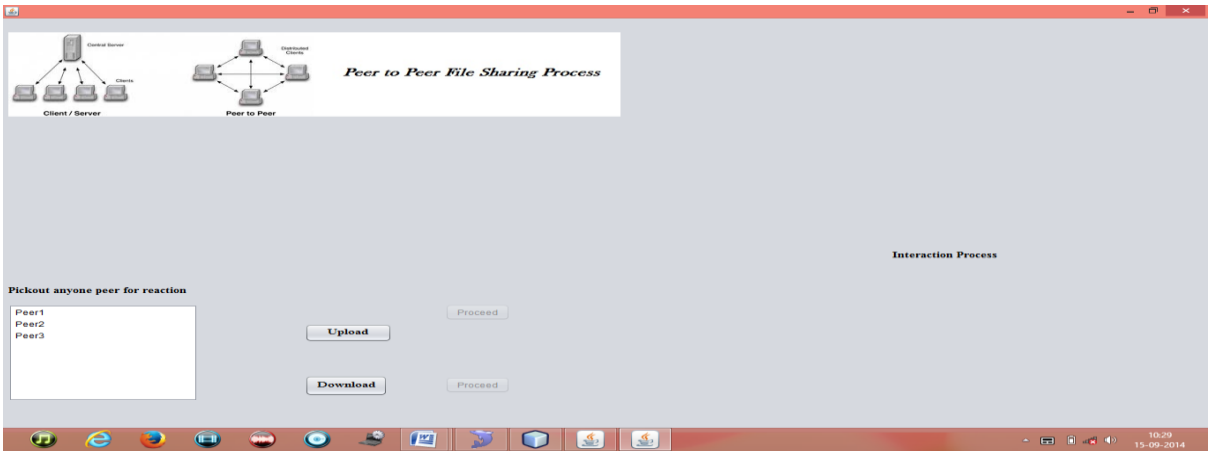
In this module, we create the interaction process between each peers. The peer which wants the file cannot download it without requesting permission from the uploaded. The peer will request to the uploader with the full details, such as filename etc. The request will be received to the uploader and then its processes. If the uploader sends the file, then only the peer can download it. With the uploader permission, the peer cannot download it. In this way the peer interaction process module takes place

4. RECOMMENDATION

In this module, the recommendation is made to the other peers regarding the service or uploader. A peer may be a good service provider but a bad recommender or vice versa. Thus, SORT considers providing services and giving recommendations as different tasks and defines two contexts of trust: service and recommendation contexts. Information about past interactions and recommendations are stored in separate histories to assess competence and integrity of acquaintances in these contexts.Using a service of a peer is an interaction, which is evaluated based on weight (importance) and recentness of the interaction, and satisfaction of the requester. An acquaintance's feedback about a peer, recommendation, is evaluated based on recommender's trustworthiness. It contains the recommender's own experience about the peer, information collected from the recommender's acquaintances, and the recommender's level of confidence in the recommendation

V. SCREEN SHOTS

HOMEPAGE

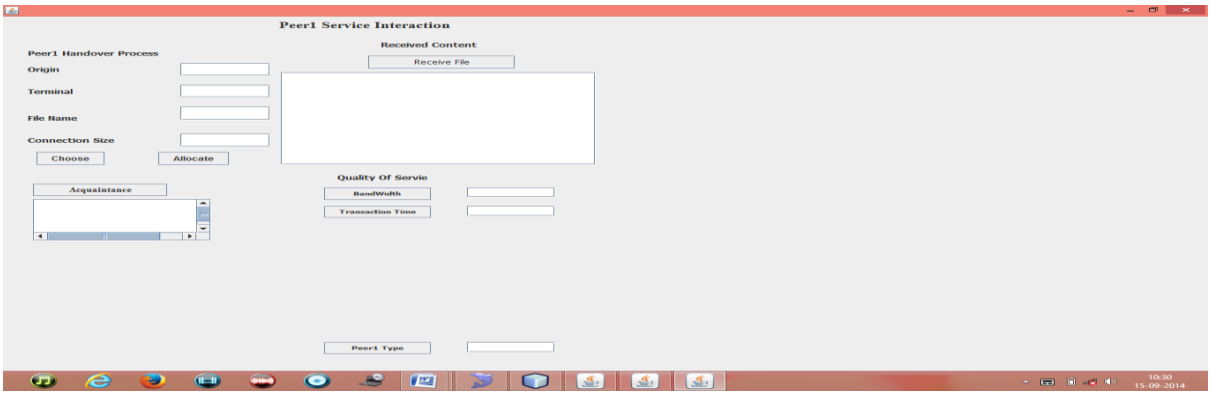


International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

DESCRIPTION

The home page depicts the file sharing process.we need to choose the peers for interaction process .The peers choosen for interaction indicate source and destination respectively.here the type of the service i.e uploading or downloading must be selected

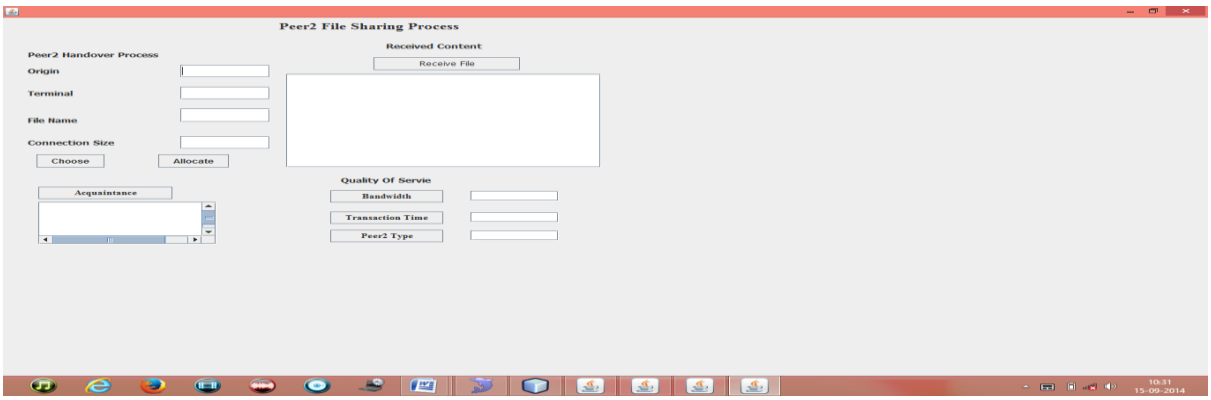
PEER INTERACTION PAGE



DESCRIPTION

In peer interaction page we need to choose the file that is to be uploaded.we can determine various factors pertaining to quality of service such as bandwidth ,transaction time,peer type.we can know the aquitances

PEER INTERACTION PAGE

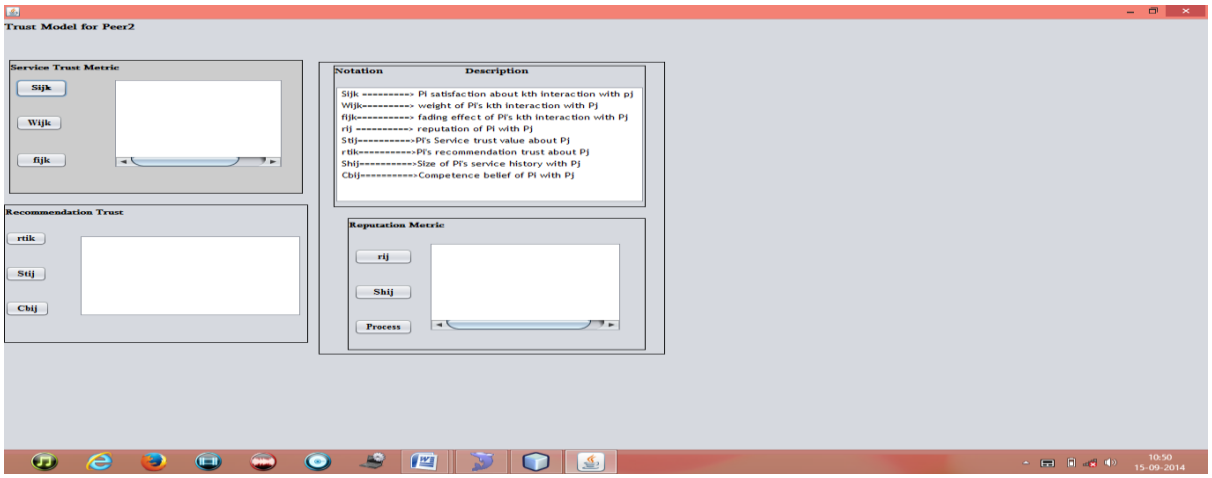


DESCRIPTION

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

In peer interaction page we need to choose the file that is to be uploaded.we can determine various factors pertaining to quality of service such as bandwidth ,transaction time,peer type.we can know the aquitances

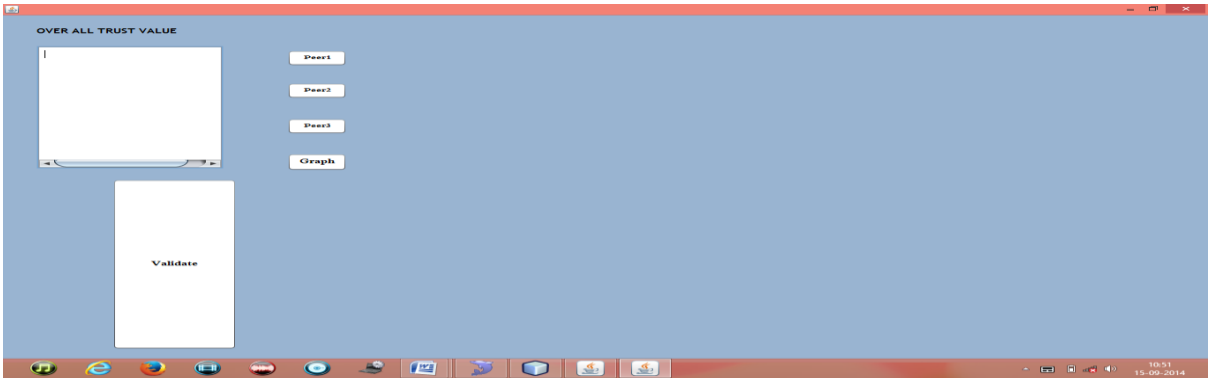
TRUST MODEL PAGE



DESCRIPTION

In trust model page various trust metrics related to service and recommendation and reputation contexts ae calculated in order to assess the trustworthiness of peers

TRUST VALIDATION PAGE

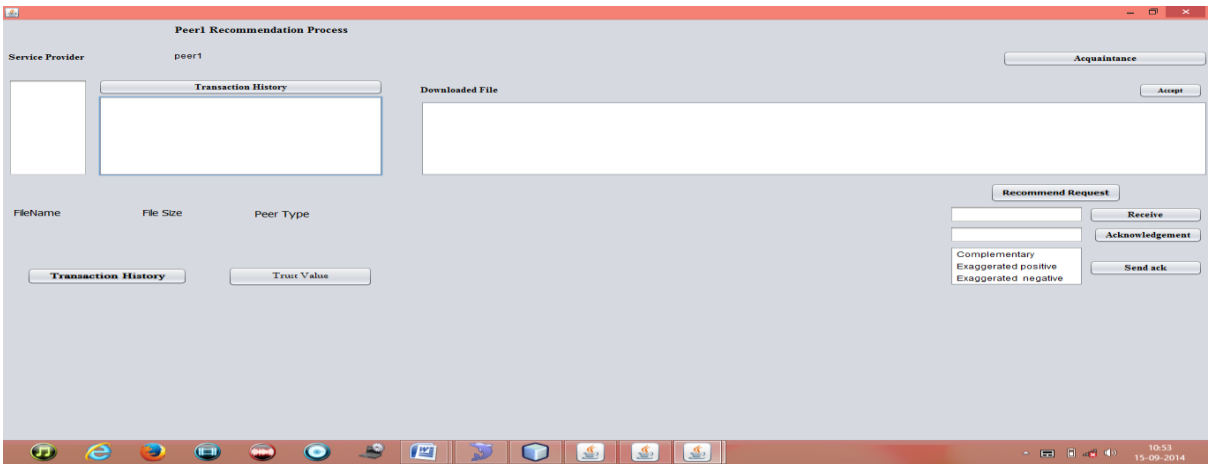


DESCRIPTION

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

Here the overall trust value for different peers is calculated and the trust value is validated by the means of a graph

RECOMMENDATION PAGE



DESCRIPTION

Here recommendation requests are sent and received.trust value pertaining to a peer as well as transaction history can be viewed.acknowledgements regarding services provided as well as recommendations about different peers can be sent and received. uploaded files can be viewed

7.CONCLUSION AND LIMITATIONS

A trust model for P2P networks is presented, in which a peer can develop a trust network in its proximity. A peer can isolate malicious peers around itself as it develops trust relationships with good peers. 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 recommender's own experience, information from its acquaintances, and level of confidence in the recommendation. These parameters provided us a better assessment of trustworthiness. Individual, collaborative, and pseudonym changing attackers are studied in the experiments. Damage of collaboration and pseudospoofing is dependent to attack behavior. Although recommendations are important in hypocritical and oscillatory attackers,

pseudospoofers, and collaborators, they are less useful in naive and discriminatory attackers. SORT mitigated both service and recommendation-based attacks in most experiments. However, in extremely malicious environments such as a 50 percent malicious network, collaborators can continue to disseminate large amount of misleading recommendations. Another issue about SORT is maintaining trust all over the network. If a peer changes its point of attachment to the network, it might lose a part of its trust network. These issues might be studied as a future work to extend the trust model. Using trust information does not solve all security problems in P2P systems but can enhance security and effectiveness of systems. If interactions are modeled correctly, SORT can be adapted to various P2P applications, e.g., CPU sharing, storage networks, and P2P gaming. Defining application specific context of trust and related metrics can help to assess trustworthiness in various tasks.

9.BIBILIOGRAPHY

[1]. Aberer and Z. Despotovic, "Managing Trust in a Peer-2-PeerInformation 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-BasedTrust 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-BasedTrust Management System for P2P Networks," Proc. IEEE/ACM Fourth Int'l Symp. Cluster Computing and the Grid (CCGRID), 2004.

[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] J. Kleinberg, "The Small-World Phenomenon: An Algorithmic Perspective," Proc. 32nd ACM Symp. Theory of Computing, 2000.[8] S. Saroiu, P. Gummadi, and S. Gribble, "A Measurement Study ofPeer-to-Peer File

Sharing Systems," Proc. Multimedia Computing and Networking, 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," IEEE Internet Computing, vol. 6,no. 1, pp. 50-57, Jan. 2002.

[10] 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.

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

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

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

[14] 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.

[15] 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.

[16] E. Terzi, Y. Zhong, B. Bhargava, Pankaj, and S. Madria, "An Algorithm for Building User-Role Profiles in a Trust Environment,"Proc. Fourth Int'l Conf. Data Warehousing and Knowledge Discovery (DaWaK), vol. 2454, 2002.

[17] Y. Zhong, "Formalization of Dynamic Trust and Uncertain Evidence for User Authorization," PhD thesis, Dept. of Computer Science, Purdue Univ., 2004.

[18] D.H. McKnight, "Conceptualizing Trust: A Typology and E-Commerce Customer Relationships Model," Proc. 34th Ann. Hawaii Int'l Conf. System Sciences (HICSS), 2001.

[19] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman,"Reputation Systems," Comm. ACM, vol. 43, no. 12, pp. 45-48,2000.

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