ISSN:0975-9646

Survey on Trust Models in Peer to Peer File Sharing Systems

Aswani Ashok, Jayakumar T V

Department Of Computer Science and Engineering
Vidya Academy of Science And Technology, Calicut University.
Thrissur,Kerala-India

***Abstract*— BitTorrent is the Peer-to-Peer(P2P) file sharing protocol mostly used nowadays. In P2P file sharing systems peers (members) communicate directly with one another to exchange information or share music, pictures, and video.P2P file sharing systems are subject to many security risks. Trust is the important factor in peer to peer file sharing systems to improve the interaction among peers and reduce malicious uploads. Survey on the different trust methods are discussed in this paper.**

***Keywords*— Peer –to- Peer network, File sharing, Trust.**

I. INTRODUCTION

BitTorrent is a communications protocol for peer-to-peer file sharing and that is used to distribute large amounts of data over the Internet. It provides download large files with high speed. [1]According to Application Usage and Threat Report of February 2013, BitTorrent was responsible for 3.35% of all worldwide bandwidth, more than half of the 6% of total bandwidth dedicated to file sharing. BitTorrent differentiates between two types of peers: leeches and seeds. Leeches are peers that only have some or none of the data while seeds are peers that have all the data but reside in the network to let other peers download from them. Thus seeds only perform uploading while leeches download files that they do not have and upload files that they have. Seeding fake files on BitTorrent is the major security threat in Torrent. Trust management systems (TMS) [7] were introduced to solve these problems. TMS assign to each peer a trust score that can be used by other peers to decide whether or not to interact with that peer. The trust score computation is based on the interaction of peers with others. Therefore, many trust and reputation management systems have been proposed to prevent attacks on P2P file sharing systems.

Fully decentralized P2P systems have no centralized mechanism, such as central servers and super nodes, to provide services to others or coordinate the operations of the systems. 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. Recognizing and isolating malicious peers is significant in all P2P environments. Therefore, many trust and reputation management systems, have been proposed to prevent such attacks on P2P systems.

The paper is divided into sections. Section 2 describes various attacks in peer to peer systems. Section 3 describes the comparison of various trust methods and section 4 concludes the survey.

II. ATTACKS

Peers participating in the trust model system may distort the trust values in various ways. It can done isolated or in cooperation with others. [2] Reputation attacks or misbehaviour of peers can be classified in the following three main categories:

(i) Unfair recommendations: Peers can spread unfair ratings for other peers or can do it with cooperation with each other to maximize the effect of the attack.
(ii) Inconsistent behaviour: Peers may strategically have an inconsistent behaviour that can lead to an incorrect estimation of their reputation allowing them to misbehave and still keep a high reputation. They can, misbehave part of the time or towards a subset of peers or change their behaviour suddenly or periodically.
(iii) Identity management related attacks: A deciding factor for attacks in this category is the identity scheme used in a reputation system. The identity scheme permits the use of multiple identities by the same peer, a malicious peer can have a dishonest behaviour and then escape its low reputation by entering the system with a new identity.

III. TRUST MODELS

Reputation-based trust management systems provide a mechanism, by which a peer requesting a resource may evaluate the trust in the reliability of the resource and the peer providing the resource. Sharing knowledge between peers is one of the ways to make at least some trust among peers. The trust management model uses a reputation trust mechanism system to evaluate trust. In reputation mechanism system, each peer may record information on past experience with all peers it has interacted with and the opinion regarding the peers that have the requested file. [3]The life cycle of a peer in a Trust management model based P2P system includes (i)Send request for a file (ii) Receive a list of peers that have the requested file (iii) Select a peer based on a Trust metric (iv) Check the access permission (v) Access the file (vi) Send feedback and update the reputation data. Trust values are estimated locally and globally. The global values calculated by

special peers. Every peer estimates personalized reputation values for other peers, based on its experience with other peer during transactions. In this way, one peer has different reputation in different peer's database, based on real life interactions.

In a decentralized reputation system the participating entities play interchangeably the roles of trustor, trustee and recommender. The trustor is an entity which wants to make a trust decision regarding whether to participate or not in a transaction with another entity, the trustee. A transaction can involve accessing or allowing access to a resource, e.g. a file, buying or selling goods, etc. The recommender is the entity that provides the trustor with information regarding the trustworthiness of the trustee; this information is known as recommendation. In file sharing P2P applications, recommendations may also be given for objects, e.g. files; reputation of objects may be estimated to help trust decisions about which object is authentic and thus it can be chosen when a particular object is required.

Trust values are estimated either locally and subjectively by the trustor or as global values calculated by special peers. In the first case every peer estimates personalized reputation values for other peers, based on its own opinions and selected recommendations from third parties. In this way, one peer has different reputation in different peers' database, as it happens in real life interactions. In the latter case, a unique global reputation value is estimated for each peer in the network, based on the opinions from the whole peer population. Local reputation values are stored by the trustor itself, whereas for global reputation values storing peers ,i.e. peers storing the reputation values, randomly or by using various techniques, such as Bloom filters or a Distributed Hash Table (DHT).

[4] The first trust algorithm designed by Aberer and Despotovic is to identify dishonest peers by a complaint based system. The disadvantage of this algorithm is that, it can't provide any means for a trustworthy peer to the distinguished a new peer, only the negative feedbacks is maintained. Its trust evaluation is very simple, distinguish every peer either as trustworthy or untrustworthy. [6] The Eigen trust algorithm is performed as, the trust value of one peer is computed by some other peers. The global reputation of each peer is marked by the local trust values assigned to the peer by other peers, and it is weighted by the global reputation of the assigned peers. The disadvantage of this method is that, it is difficult to identify the new peers. [5] In Peer Trust method each peers trust is calculated based on some parameters. The parameters for trust evaluation are (i) The feedback a peer obtains from other peers (ii) The feedback scope, such as the total number of transactions that a peer has with other peers(iii) The credibility factor for the feedback source (iv) The transaction context factor for discriminating mission-critical transactions from less or noncritical ones, and (v) The community context factor for addressing community related characteristics and vulnerabilities. But it does not provide any mechanism that can completely prevent the attack of peers being compromised.

The Power Trust[8] system dynamically selects small number of power nodes that are most reputable using a distributed ranking mechanism. It collects locally generated peer feedbacks and aggregates them to yield the global reputation scores. Calculated trust information is not a global trust value and does not reflect opinions of all peers. [7] The trust management system for BitTorrent uses global trust scores as well as local trust scores. Each peer assigns a trust score to each of its neighbours and the tracker of each BitTorrent maintain global trust scores. [10] In Gossip Trust uses gossip protocol and the techniques used in [8] Power Trust. It is suited only for small applications. [9] Ahmet Burak Can and Bharat Bharagava et al propose a Self-ORganizing Trust model (SORT) aims to decrease malicious activity in a P2P system by establishing trust relations among peers. Peers uses distributed algorithms to find the trustworthiness of other peers based on the available local information which includes past interactions and recommendations received from others. Peers collaborate to establish trust among each other without using a priori information or a trusted third party. [11] Predictability Trust based on two key concepts: Predictability Trust and Dynamic Sliding Windows. Predictability Trust works with some other type of trust to detect attacks and uses sliding windows (SWs) to keep track of previous behaviors so that it can determine how quickly to redeem trust.

BitTorrent does not offer its users anonymity nor security. It is possible to obtain the IP addresses of all current and possibly previous participants in a swarm from the tracker. This may expose users with insecure systems to attacks. It may also expose users to the risk of being used, if they are distributing files without permission from the copyright holders.

IV. CONCLUSIONS

Peer-to-Peer systems offer many advantages for free sharing of resources between users. But it is difficult to incorporate trust between the users. The malicious peers spread inauthentic files that might disrupt the entire system. Therefore, reputation management systems are emerging to overcome this problem.

REFERENCES

[1] "Application Usage & Threat Report". An Analysis of Application Usage and Related Threats within the Enterprise,10th Edition, February 2013.

[2] Yu Yang and Lan Yang, "A Survey of Peer-to-Peer Attacks and Counter Attacks," CSE Department, California State Polytechnic University, Pamona.

[3] A. Amuthan, Marimuthu G, Kaliaperumal G. "Secure Trust Management Model for Peer-to-Peer File Sharing System". ACEEE International Journal on Network Security, 2011, 2 (1),pp.7.

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

[5] 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.

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

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

[8] R. Zhou and K. Hwang,” Powertrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing”,,IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 4, pp. 460-473, Apr, 2007.

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

[10] 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.

[11] Younghun Chae, Lisa Cingiser DiPippo, Yan Lindsay Sun,” Trust Management for Defending On-Off Attacks” IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 4, APRIL 2015

[12] Tamilmani, Karthik (25 October 2003). "Studying and enhancing the BitTorrent protocol". Stony Brook University. Archived from the original (DOC) on 19 November 2004. Retrieved 6 May 2006