International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Group Formation with Neighbour Similarity Trust in P2P E-Commerce

M. Robin Rutherford[1], V. Dheepa[2]

[1]Department of Computer Science and Engineering, Hindustan University, Padur

[2]Assistant Professor, Department of Computer Science and Engineering, Hindustan University, Padur

Abstract: ***This paper is based on networking in predicting the trust between Peer to peer (P2P) e-commerce applications with liabilities to passive and active attacks. These attacks have turned out the potential business firms and individuals whose aim is to get the best benefit in e-commerce with minimal losses. The attacks occur when contacts between the swapping peers as an execution occurs In this paper, Sybil attack is proposed as an active attack, in which peers can have asserts, and can be considered as numerous identities to fake their owns. In our approach, traced Sybil attack peers can be recognized as the adjacent peers and became more trusted to each other. Security and performance analysis shows that Sybil attack can be reduced by our proposed neighbour similarity trust. The peer identities are then occupied to drag the behaviour of the system. However, if a single flawed entity can present multiple identities, it can control a massive proportion. All the resources utilized in the P2P infrastructure are contributed by the peers itself unless a traditional approaches where a central authority control is used. A peer gives illegal tributes will have its trust level minimised. In case it reaches a certain threshold level, the peer can be expelled from the group. Each peer has an identity, which is either honest or Sybil.***

Keywords: P2P; trust; Sybil attack; collusion attack; neighbor similarity.

1. Introduction

Each and every peer plays the dualistic role of client and server, which means that each has its own control. All the resources utilized in the P2P infrastructure are confronted as the peers it selves unless the traditional approach that uses central authority control. Peers can collide and can do all sorts of mischevious activities in the open-access distributed systems. These malicious behaviours lead to service quality reduction and economic loss among business forces. Peers are vulnerable to manipulation, due to the open and near zero cost of molding new identities. The goal of trust systems is to warrant that honest peers are precisely identified as authorized and Sybil peers as untrustworthy. For our convenient we call identities created by unauthorized users as Sybil peers. In a P2P e-commerce application scenario, most of the trust considerations depend on the historical reasons of the peers. The influence of Sybil identities can be reduced based on the historical behaviours and recommendations from other peers. For example, a peer can give positive recommendations to a peer which is discovered as a Sybil or malicious peer. This can demolish the influence of Sybil identities hence by reducing Sybil attack. A peer which has been giving dishonest approvals will have its trust level greatly reduced. In case it reaches a certain threshold level, then the peer can be expelled from the group. A Sybil identity can be an identity owned by a malicious user, or it can be a bribed/stolen identity, or it can be a fake identity obtained through a Sybil attack[24]. These Sybil attack peers are employed to target honest peers and hence suppress the system. In Sybil attack, a single malicious user creates a large number of peer identities called Sybil's. These Sybil's are used to send forth security attacks, both at the application level and at the overlay level [18]. At the application level, Sybil's can target other honest peers while auctioning with them, whereas at the overlay level, Sybil's can intrude the services offered by the overlay layer like routing, data storage, lookup, etc. In trust systems, Withstanding against Sybil attack is quite a challenging task. A peer can represent to be trusted with a hidden motive. The peer can contaminate the system with bogus information, which interferes with genuine business transactions and functioning of the systems [6]. This must be counter prevented to guard the honest peers. The link between an honest peer and a Sybil peer is known as an attack edge. As each edge resembles a human-established trust, it is difficult for the antagonist to introduce an excessive number of attack edges. The only known promising defines against Sybil attack is to use social networks to perform user admission control and limiting the number of bogus identities admitted to a system The use of social networks between two peers represents real-world trust conjunction between users. In addition, authentication-based mechanisms are used to validate the identities of the peers using shared encryption keys, or location information. Most existing work on Sybil attack makes use of social networks to compress Sybil attack, and the findings are based on pretending Sybil identities. In this paper, profound the use of neighbour parallel trust in a group of P2P e-commerce which is based on interest links, to eliminate among the peers. This is referred to as Sybil Trust. In Sybil Trust, the interest based group infrastructure peers have a neighbour similarity trust between each other, hence they are able to prevent Sybil attack. Sybil Trust gives a better relationship in e-commerce communications as the peers create a communication between peer neighbours. This provides an important channel for peers to advertise their products to other interested peers and to know new market targets and contacts as well. In addition, the group enables a peer to join P2P e-commerce network and makes identity more competitive.. Peers use self-certifying identifiers that are ex-changed when they comes into contact. These can be used as public keys to validate digital signatures on the messages sent by their neighbours. Note that, all transactions between peers are digitally signed. This kind of links, use neighbours as our point of reference to address Sybil attack. In a group, whatever rights of entry we activate, there are honest,

malicious, and Sybil peers who are verified by an admission control mechanism to join the group. Large honest peers are admitted compared to maluscious peers, where the trust force is aimed at positive results. The knowledge of the graph may set in a single party, or distributed across all users. In our work, Use the distributed admission control that needs each peer to be initially aware of its immediate trusted and honest neighbours. The neighbours relieve to finalise other peers of same interest in different levels. In this paper, we present a distributed designed approach to Sybil attack. This is extracted from the fact that this approach is based on the neighbour similarity trust links among the neighbour peers. Given a P2P e-commerce trust relationship, the transactions among peers are reliable as each peer can decide to trade with other. A peer doesn't have to receive choice of others in a group unless assistance is needed. It shows the advantage in exploiting the concurrency in trust relationships among peers in which they are able to monitor each other. The contribution in this paper is threefold

1) Sybil Trust is proposed that can identify and pretend honest peers from Sybil attack. The Sybil peers can have their trust cancelled and disconnected from a group.
2) Based on the group infrastructure in P2P e-commerce, each neighbour is linked to the peers by the success of their links it makes or the trust evaluation level. A peer can only be perceived as a neighbour related to it on whether or not trust level is sustained over a threshold value.
3) Sybil Trust enables neighbour peers to hold recommendation identifiers among them in a group. This preserves that the group detection algorithms to identify Sybil attack peers is efficient and scalable in large P2P e-commerce networks.

To achieve these results, Sybil Trust uses a distributed algorithm to function the neighbour verification to make sure that the neighbour similarity trust information is kept as honest and integrity is maintained as possible. Sybil Trust is able to limit the number of admitted controlled Sybil attack peer identities to a very small number while admitting most honest identities. After we admit a number of attack edges to cover more peers, the number of admitted Sybil attack peer identities remains very low. In this paper, note that 1) the Sybil attack peers tend to be poorly connected to the rest of the network, compared to the honest peers, and 2) the Sybil attack peers use various graph analysis techniques to search for topological features resulting from their limited capacity to establish neighbour similarity links.

2. System Description and Models

2.1 Network Model

Consider a group with a number of peers which have open and anonymous characteristics. A peer cannot make its own decisions on trust to another peer unless it is a member of the group. Each peer relates to other peers depending on the trust it has. A graph G is a tuple h*V, E* i, where V is a set of |V | = n vertices and E is a set of edges. Specifically, $V = \{v_1, v_2, \cdots, v_x\}$ represents the peers available, and $E = \{e_1, e_2, ..., e_y\}$ represents the edges among the peers. An edge is an ordered pair (v, z) of vertices, where v is called a trustor, and z is called a trustee. If vertex z is adjacent to vertex v, there is an edge (v, z) in E from v to z. Notice that if there is an edge (v, z) in E, then there is also an edge (z, v) in E.The neighborhood of a peer v in a P2P e-commerce is N (v) = {z/(v, z) ∈ E}. Each peer v maintains a set of identifiers of its neighbors N (v), in which each one is unique. Messages can be sent from a peer v to a peer z, provided that v knows the identifier of z. Any packet broadcast by a peer is received by all its neighbors.

2.2 Attack Model

In order to launch a Sybil attack, a malicious peer must try to present multiple distinct identities. This can be achieved by either generating legal identities or by impersonating other normal peers. Some peers may launch arbitrary attacks to interfere with P2P e- commerce operations, or the normal functioning of the network. According to [4] an attack can succeed to launch a Sybil attack by:

- *Heterogeneous configuration*: in this case, malicious peers can have more communication and computation resources than the honest peers.
- *Message manipulation*: the attacker can eavesdrop on nearby communications with other parties. This means a attacker gets and interpolates in- formation needed to impersonate others.

Major attacks in P2P e-commerce can be classified as passive and active attacks.

- *Passive attack:* It listens to incoming and outgoing messages, in order to infer the relevant information from the transmitted recommendations, i.e., eavesdropping, but doesn't harm the system. A peer can be in passive mode and later in active mode.
- *Active attack:* When a malicious peer receives a recommendation for forwarding, it can modify, or when requested to provide recommendations on another peer, it can inflate or bad mouth. The bad mouthing is a situation where a malicious peer may collude with other malicious peers to revenge the honest peer. In the Sybil attack, a malicious peer generates a large number of identities and uses them together to disrupt normal operation.

In this paper, the active attacks is focused in P2P e-commerce. When a peer is compromised, all the information will be extracted. In this paper, Sybil Trust is proposed which is based on neighbor similarity relationship of the peers. Sybil Trust is efficient and scalable to group P2P e-commerce network.

3. Preliminaries

3.1 Neighbor Similarity Trust

Sybil detection algorithm that takes place in a neighbor similarity trust. The directed graph G = (V, E) has edges and vertices. Assume V is the set of peers and E is the set of edges. The edges in a neighbor similarity have attack edges

which are protected from Sybil attacks. A peer u and a Sybil peer v can trade whether one is Sybil or not. Being in a group, contrast can be done to find out the number

3.2 Cooperation among Peers in a Neighbourhood

Mutual effort is the plan of a group of entities working collected to achieve a common or individual target. Mutual effort can be seen as an exploit of tracking down some advantage by giving, sharing, or given something. In mutual effort assume all the members gain. Among the peers, there are hateful and greedy peers which don't collaborate with others. In this investigate, note the connection between thinking over reviewing peer and a peer being compared is value seeking for similarity. It can help the regard model decrease hateful opinion, collect more personal opinion, and finally workout the universal trust value. A neighborhood need to have motives tendered to the peers in order to inspire them to mutual effort. In P2P we can classify motives ideas into neighbor correlation-based system and paying-based system. Mutual effort aims to decrease plan peers which to begin with act well and get high trust value after piecing together a network. Later, they start to behave faithlessly lowering QoS and as long as lying comment. The P2P neighbor similarity activity must be a joint trust level relation. Comment valuation among the peers is normally in deal with service valuation. Honest nodes provide honest facilities and comment, while untrust nodes provide neither honest facilities nor honest comment whether they have a similar correlation or not.

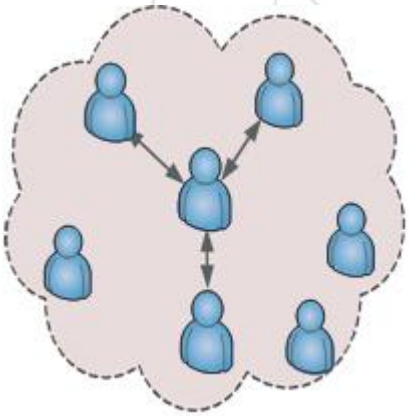

Figure 1: Detection of Sybil attack

3.3 Detection of Sybil Attack Based on Neighbour Similarity Trust

In Sybil attack, each malicious peer will forge mul- tiple identity which does not physically exist within a network, in order to mislead the legitimate peers and honest peers into believing that they have many neighbors [8]. In this paper, assume there are three kinds of peers in the system: legitimate peers, malicious peers, and Sybil peers. Each malicious peer cheats its neighbors by creating multiple identity, referred to as Sybil peers. In this paper, P2P e-commerce communities are in several groups.

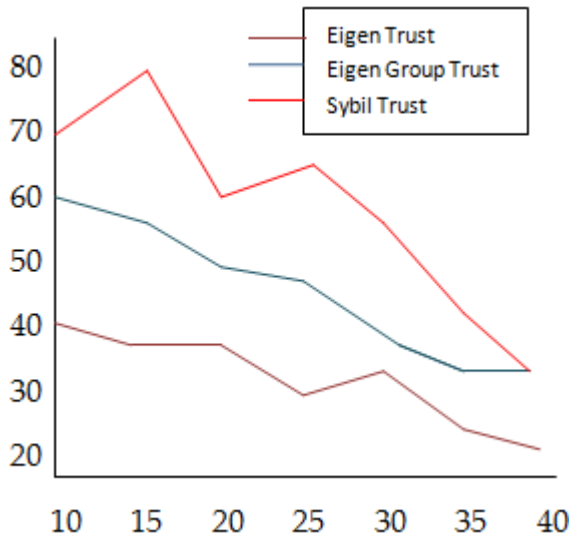

Figure 2: Percentage of peers that detected the mailicious peer

A group can be either open or restrictive depending on the interest of the peers. Investigate the peers belonging to a certain interest group. In each group, there is a group leader who is responsible for managing coordination of activities in a group [27]. When peers join a group, they acquire different identities in reference to the group. Each peer has neighbors in the group and outside the group. Sybil attack peers forged by the same malicious peer have the same set of physical neighbors that a malicious peer has. Each neighbor is connected to the peers by the success of the transaction it makes or the trust evaluation level. To detect the Sybil attack, where a peer can have different identity, a peer is evaluated in reference to its trustworthiness and the similarity to the neighbours. If the neighbours do not have same trust.

4. Security Analysis

Illustrate the Sybil Trust resilience by use of the controller in the peers to show that each controller only admitted the honest peers. Our method makes assumptions that the controller undergoes synchronization to prove whether the peers which acted as distributor of identifiers had similarity or not. If a peer never had similarity, the peer is assumed to have been a Sybil attack peer. Pairing method is used to generate an expander graph with expansion factor of high probability. Every pair of neighbor peers share a unique symmetric secret key, established out of band [8] for authenticating each other. A Sybil attack peer may disclose its edge key with some honest peer to another Sybil attack peer. However, because all neighbors are authenticated via the edge key, when A sends a message to B, B will still route the message as if it comes from B. In the protocol, every peer has a pre-computed random permutation (being the peer 's degree) as its routing table. The routing table never changes unless the peer adds new neighbors, or deletes old neighbors. A random route entering via edge always exits via edge.

5. Conclusion

Sybil Trust, a protection opposed Sybil attack in P2P e-commerce. Evaluated to other approaches, this approach is based on neighborhood similarity trust in a group P2P e-commerce society. This approach efforts the connection between peers in a neighborhood setup. On real-world P2P e-commerce complete fast-mixing proprietary, hence approved the fundamental supposition at the back Sybil- Guard's approach. Also describe guard types such as key validation, distribution, and position verification. This systems can be done at the same time with neighbor similarity trust which gives better defense mechanism. Neighbor similarity trust helps to sweep out the Sybil peers and close-off hatefulness to particular Sybil peer groups pretty than agree attack in honest groups with all honest peers.

References

[1] J. Douceur, "The Sybil Attack, " Proc. of IPTPS, 2002, pp. 251-260.
[2] A. Mohaisen, N. Hopper, and Y. Kim, "Keep your Friends Close: Incorporating Trust into Social Network-based Sybil Defenses, " Proc. of IEEE INFOCOM, 2011, pp. 1-9.
[3] K. Walsh and E. G. Sirer, "Experience with an Object Reputation System for Peer to Peer Filesharing, " Proc. of USENIX NSDI,2006, pp. 1-14.
[4] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks, " IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 6, June 2012, doi:10.1109/TPDS.2011.263, pp. 1103-1114.
[5] B. Yu, C.Z. Xu, and B. Xiao, "Detecting Sybil attacks in VANETs," Journal of Parallel and Distributed Computing (JPDC - Elsevier), Vol. 73, No. 3, June 2013, Pp. 746-756.
[6] T. Nguyen, L. Jinyang, S. Lakshminarayanan, and S. M. Chow, "Optimal Sybil-Resilient Peer Admission Control," Proc. of IEEE INFOCOM, 2011, pp. 3218-3226.
[7] K. Wang, M. Wu, and S. Shen, "Secure Trust-Based Cooperative Communications in Wireless Multi-hop Net- works,"Communications and Networking, Book chapter 18, Book edited by: Jun Peng, September 2010, ISBN 978-953-307-114-5, pp. 360-378.
[8] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao, "SybilLimit: A Near-Optimal Social Network Defense against Sybil Attack," IEEE/ACM Transactions on Networking, Vol. 18, No. 3, June 2010, pp. 3-17.
[9] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybil- Guard: Defending against Sybil Attack via Social Networks," IEEE/ACM Transactions on Networking, Vol. 16, No. 3, June 2008, pp. 576-589.
[10] A. Tversky, "Features of Similarity, " Psychological Review, Vol.84, No. 2, 1977, pp. 327-352.
[11] F. Musau, G. Wang, and M. B. Abdullahi, "Group Formation with Neighbor Similarity Trust in P2P E-Commerce," Proc. of Joint Conference of IEEE TrustCom/IEEE ICESS/FCST, November2011, pp. 835-840.
[12] G. Danezis and P. Mittal, "SybilInfer: Detecting Sybil Attack Peers using Social Networks," Proc. of NDSS, San Diego, CA, February 2009, pp.1-15.
[13] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses," Proc. of IPSN, ACM, April 2004, pp.1-10.
[14] W. Wei, X. Fengyuan, C. T. Chiu, and L. Qun, "SybilDefender: Defend Against Sybil Attacks in Large Social Networks," Proc. of IEEE INFOCOM, 2012, pp.1951-1959.
[15] L. Xu, S. Chainan, H. Takizawa, and H. Kobayashi, "Re- sisting Sybil Attack by Social Network and Network Clus- tering," International Symposium on Applications and the Internet IEEE/IPSJ SAINT, 2010, pp.15 - 21
[16] N. Tran, B. Min, J. Li, and L. Subramanian, "Sybil-Resilient Online Content Voting," Proc. of the 6th USENIX, Symposium on Networked Systems Design and Implement, USENIX Association, 2009, pp. 15-28.
[17] I. Stoica, R. Morris, D. Karger, F. Kaashoek, and H. Balakr- ishnan, "Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications," Proc. of ACM SIGCOMM, 2001, pp. 149-160.
[18] B. S. Jyothi and D. Janakiram, "SyMon: A Practical Approach to Defend Large Sstructured P2P systems against Sybil At- tack," Springer Science+Business Media, LLC 2010, pp.