Volume 6, Issue 2, February 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Centrally Organized Neighbor Similarity Trust against Sybil Attack in P2P E-Commerce

[1]Urvashi Tripathy, [2]Professor Shriram Yadav

[1] M.tech Scholar, CSE, Millenium Institute of Technology & Science RGPV, India

[2] Guide & Head, P.G.CSE, Millenium Institute of, Technology & Science, India

Abstract- Peer to peer (P2P) e-commerce applications exist at the edge of the Internet with vulnerabilities to passive and active attacks. These approaches have pushed away potential business firms and individuals whose aim is to get the best benefit in e-commerce with minimum losses. The attacks occur during interactions between the trading peers as a transaction takes place. One practical limitation of peer-to-peer (P2P) networks is that they are often subject to Sybil attacks: malicious parties can compromise the network by generating and checking large numbers of shadow identities. In this report, we suggest how to address the Sybil attack, an active attack, in which matches can have bagels and multiple identities to fake their own. Most existing work, which focuses on social networks and trusted certification, has not been able to prevent Sybil attack peers from doing proceedings. Our work exploits the neighbor similarity trust relationship to address the Sybil attack. In our approach, duplicated Sybil attack peers can be identified as the neighbor peers become acquainted and hence more trusted in each other. Security and performance analysis shows that Sybil attack can be minimized by our proposed neighbor similarity trust.

Keywords- p2p, trust, Sybil attack, collusion attack.

I. INTRODUCTION

Sybile attacks, where a single entity emulates the behavior of multiple users, make a fundamental threat to the protection of distributed systems. Example systems include peer to peer networks, email, reputation systems, and online social networks. For instance, in 2012 it was reported that 83 million out of 900 million Facebook accounts are Sybil's. Sybil accounts in online social networks are used for criminal activities such as spreading spam or malware, stealing other users' private information and manipulating web search results via "+1" or "like" clicks.

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 subvert 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 launch 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 transacting with them, whereas at the overlay level, Sybil's can disrupt the services offered by the overlay layer like routing, data storage, lookup, etc. In trust systems, colluding Sybil peers may artificially increase a (malicious) peer's rating (e.g., eBay). Systems like Credence [3] rely on a trusted central authority to prevent malicious.

P2P networks range of communication systems like email and instant messaging to collaborative content rating, recommendation, and delivery systems such as YouTube, Gnutela, Facebook, Digg, and Bit Torrent. They allow any user to join the system easily at the expense of the trust, with very little validation control. P2P overlay networks are known for their many desired attributes like openness, anonymity, decentralized nature, self-organization, scalability, and fault tolerance [18]. Each peer plays the dual role of the client as well as server, meaning that each has its own control. All the resources utilized in the P2P infrastructure are contributed by the peers themselves, unlike traditional methods where a central authority control is used. Peers can collude and do all sorts of malicious activities in the open-access distributed systems. These malicious behaviors lead to service quality degradation and monetary loss among business partners. Peers are vulnerable to exploitation, due to the open and near-zero cost of creating new identities. The peer identities are then utilized to influence the behavior of the system. However, if a single defective entity can present multiple identities, it can control a substantial fraction of the system, thereby undermining the redundancy [1].

The number of identities that an attacker can generate depends on the attacker's resources such as bandwidth, memory, and computational power [2]. The goal of trust systems is to ensure that honest peers are accurately identified as trustworthy and Sybil peers as untrustworthy. To unify terminology, we call all identities created by malicious users as Sybil peers. In a P2P e-commerce application scenario, most of the trust considerations depend on the historical factors of the peers.

The influence of Sybil identities can be reduced based on the historical behavior and recommendations from other peers. For example, a peer can give positive recommendations to a peer which is discovered is a Sybil or malicious peer. This can diminish the influence of Sybil identities hence reduce Sybil attack. A peer which has been giving dishonest recommendations will have its trust level reduced. 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.

Defending against Sybil attack is quite a challenging task. Douceur [2] was the first to consider multiple identity problems in the context of P2P networks. A peer can pretend to be trusted with a hidden motive. The peer can pollute the system with bogus information, which interferes with genuine business transactions and functioning of the systems [6]. This counter must be prevented to protect the honest peers. The link between an honest peer and a Sybil peer is known as an attack edge. As each edge involved resembles a human-established trust, it is difficult for the adversary to introduce an excessive number of attack edges. The only known promising defense against Sybil attack is to use social networks to perform user admission control and limit the number of bogus identities admitted to a system [8], [9], [12], and [14]. The use of social networks between two peers represents real-world trust relationship between users. In addition, authentication-based mechanisms are used to verify the identities of the peers using shared encryption keys, or location information.

Most existing work on the Sybil attack makes use of social networks to eliminate a Sybil attack, and the findings are based on preventing Sybil identities. In this paper, we propose the use of neighbor similarity trust in a group P2P ecommerce based on interest relationships, to eliminate maliciousness among the peers. This is refereed to as Sybil Trust. In Sybil Trust, the interest based group infrastructure peers have a neighbor similarity trust between each other, hence they are able to prevent Sybil attack. Sybil Trust gives a better relationship in e-commerce transactions as the peers create a link between peer neighbors. This provides an important avenue for peers to advertise their products to other interested peers and to know new market destinations and contacts as well. In addition, the group enables a peer to join P2P e-commerce network and makes identity more difficult. Peers use self-certifying identifiers that are exchanged when they initially come into contact. These can be used as public keys to verify digital signatures on the messages sent by their neighbors. We note that, all communications between peers are digitally signed. In this kind of relationship, we use neighbors as our point of reference to address the Sybil attack. In a group, whatever admission we set, there are honest, malicious, and Sybil peers who are authenticated by an admission control mechanism to join the group. More honest peers are admitted compared to malicious peers, where the trust association is aimed at positive results. The knowledge of the graph may reside in a single party, or be distributed across all users. In our work, we use the distributed admission control which only requires each peer to be initially aware of only its immediate trusted neighbors, and look for honest neighbors. The neighbors assist to locate other peers of the same interest in other levels. We make an important observation about the challenges of Sybil resilient peers in admission. It has been impossible to get an algorithm which can detect all Sybil attack peers and identify all the honest peers.

In this section, we describe our network model and the attack model:

Network model

We 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 V; Ehi, where V is a set of jVj¼n vertices and E is a set of edges. Specifically, V ¼f v1; v2; vxg represents the peers available, and WANG ET AL.: NEIGHBOR SIMILARITY TRUST AGAINST SYBIL ATTACK IN P2P E-COMMERCE 825

E ¼f e1; e2; eyg represents the edges among the peers. An edge is an ordered pair ðv; zÞ 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 ðv; zÞ in E from v to z: Notice that if there is an edge ðv; zÞ in E; then there is also an edge; vÞin E:

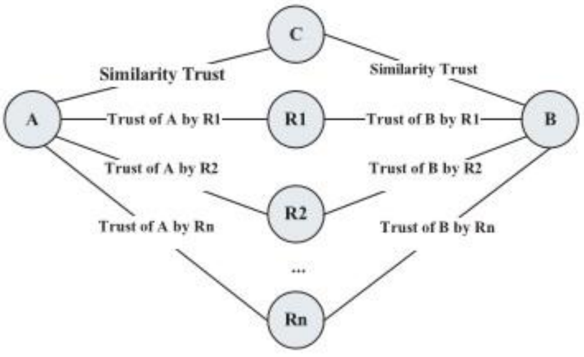

Fig 1: Neighbor similarity computational model

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 an attacker gets and interpolates information needed to impersonate others. Major attacks in P2P e-commerce can be classified as passive and active attacks.

Passive attack.

A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is solely to gain information about the target and no data is changed on the target. 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.

An active attack, in computing security, is an attack characterized by the attacker attempting to break into the system. During an active attack, the intruder will introduce data into the system as well as potentially change data within the system. 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.

II. LITERATURE REVIEW

J. Douceur [1] the security challenges of a novel perspective of VANETs, i.e., taking VANETs to clouds. We have first introduced the security and privacy challenges that VC computing networks have to face, and we have also addressed possible security solutions. Although some of the solutions can leverage existing security techniques, there are many unique challenges. For example, attackers can physic- cally locate on the same cloud server. The vehicles have high mobility, and the communication is inherently unstable and intermittent. We have provided a directional security scheme to show an appropriate security architecture that handles several, not all, challenges in VCs. In future work, we will investigate the brand-new area and design solutions for each individual challenge. Many applications can be developed on VCs.

A. Mohaisen, N. Hopper, and Y. Kim [2] we explored understanding and improving the mixing characteristics of social graphs. We pointed out that the mixing characteristics of social graphs are related to the core structure, and used that to improve the mixing time. Using a running example, we demonstrated that the improved mixing time affects Sybil defenses, such as Sybil Limit, although findings can be applied to other defenses. Although potentially addressable with current mathematical means, we will look at how theoretically the mixing time is improved by our heuristics. We want to look at how an X-c-C heuristic, by adding only c edges to the social graph, will improve its mixing characteristics.

K .Walsh [3] Credence is a new approach for combating the widespread presence of decoys, malware, and other malicious content in peer-to-peer file sharing systems. The system provides incentives for peers to participate honestly in voting, enables peers to compute object reputations that reflect their authenticity, and is robust to coordinated attacks. We have made a complete Credence implementation, with source code, freely available. Data from a long-term study of the emerging properties of the deployed network suggests that Credence users are able to identify malicious file sharing activity and mitigate the impact of dishonest peers in the Credence reputation system.

Devid coll, Jun li,Joshua stein[4] In this work, by focusing on the performance of each Sybil defense solution under the modern scenario, which more truly reflects the evolving behavior of Sybil attackers, we extensively measured and evaluated major Sybil defense schemes, and unveiled that current OSN-based Sybil defenses do contain severe weaknesses. We find that, when Sybil's are not herded together in a distinct Sybil community with very few links to the outside world, all of the evaluated schemes suffer in their effectiveness—some more than others. Sybil detection approaches, even with a modified design, have a hard time reliably distinguishing a Sybil node from honest nodes. In fact, whereas it has been shown that Sybil's can obtain

Hundreds of attack edges in real-world OSNs, our study shows all existent approaches can be circumvented by the presence of only a handful of attack edges. Sybil tolerance schemes are application-specific and rather than being fundamentally flawed, their weaknesses are mostly in the details. Nonetheless, they too are vulnerable if Sybil's vary their assumed behavior. Our study provides insights to new Sybil defense solutions. We anticipate a Sybil defense approach to be more effective if leveraging not only structural properties of an OSN, but also more information about the relations between its users.

B. Yu, C. Z. Xu, and B. Xiao [5] a method base on cryptography to detect Sybil attack in VANET. Result of simulation shown that Execution time of this algorithm is low, because most operations is done in Certification Authority, so the proposed method is a best method for detection of Sybil attacks. The simulations indicates that, delay of detection Sybil attack depends on the number of messages not to number of vehicles. In our future work we would like to discover location of malicious node, because this nodes is important problem in this type of attacks, prevents of other attacks if malicious nodes is identify. This proposed schema have a problem that, if nodes move to other rejoins, detection of Sybil attack does not work properly.

T. Nguyen, L. Jinyang, S. Lakshmi Narayan an, and S. M. Chow, [6] Gatekeeper is an optimal decentralized admission control protocol based on social networks that admits O(log k) Sybil nodes per attack edge with high probability. Our protocol improves over Sybil Limit, the best known Sybil-resilient node admission protocol by a factor of O (log n) on random expander graphs when the attacker controls only O (1) attack edges. Simulation results demonstrate that Gatekeeper works well on real-world social networks. Even in the face of a large number of attack edges, Gatekeeper can significantly limit the number of admitted Sybil nodes per attack edge.

K. Wang, M. Wu, and S. Shen [7]Trust evaluation can effectively improve network performance and detect malicious nodes, trust evaluation itself is an attractive target for attackers (Marmol & Penez, 2009). A well-known attack is bad-mouthing attack (Dellarocas, 2000), that is, malicious parties providing dishonest recommendations to frame up good parties and/or boost trust values of malicious peers. The defense against the bad-mouthing attack has been considered in the design of the proposed trust evaluation system.

III. PROPOSED METHODOLOGY

As we have studied in the current system, there is a Sybil trust level in the peer system, but still they have specified the work can be done further by maintaining a Sybil trust system in the multiple group of peer and can use to protect by several attacks which are malicious and having high dimension in the attack scenario in group of peers rather than the single network, here the technique of trust level scheme is going to monitor in the group, the efficiency and working need to monitor in our proposed

Work. The trusted authentication center in a centralized large-scale distributed system can certify each identity to defend against Sybil attacks. However, decentralized large-scale distributed systems do not have a trusted authentication center. This condition makes such systems vulnerable to Sybil attacks. We are going to make a system where we are going to make a group of peers and maintaining a central Sybil trust in order to maintain security and privacy in between the multiple peers in the network and communication.

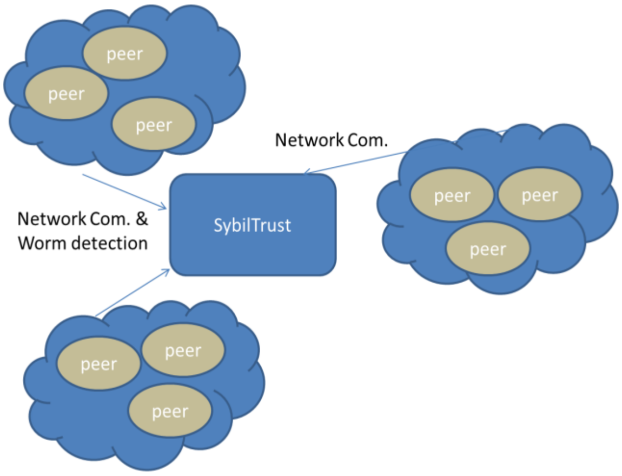

Figure- proposed work scenario

IV. CONCLUSION

Equally the work we have discussed, here we mention about the various techniques which exist along with the trusted system in Sybil and network system where the current paper discuss about the network status and problem associated with the network, as well as we have delayed the further Sybil trust can be united with the group of peer node and we face a scenario where we are starting to put on the Sybil trust center scheme in group and going to monitor the proposed study and its efficiency.

REFERENCES

[1] J. Douceur, “The Sybil attack,” in Proc. Revised Papers 1st Int. Workshop Peer-to-Peer Syst., 2002, pp. 251–260.

[2] A. Mohaisen, N. Hopper, and Y. Kim, “Keep your friends close: Incorporating trust into social network-based Sybil defenses,” in Proc. IEEE Int. Conf. Compute. Common. 2011, pp. 1–9.

[3] K. Walsh and E. G. Sirer, “Experience with an object reputation system for peer to peer files haring,” in Proc. 3rd USENIX Conf. Netw. Syst. Des. Implementation, 2006, vol. 3, pp. 1–14.

[4] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, “Footprint: Detecting Sybil attacks in urban vehicular networks,” IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 6, pp. 1103–1114, Jun. 2012.

[5] B. Yu, C. Z. Xu, and B. Xiao, “Detecting Sybil attacks in VANETs,” J. Parallel Distrib. Compute. vol. 73, no. 3, pp. 746–756, Jun. 2013.

[6] T. Nguyen, L. Jinyang, S. Lakshminarayanan, and S. M. Chow, “Optimal Sybil-resilient peer admission control,” in Proc. IEEE Int. Conf. Compute. Common. 2011, pp. 3218–3226.

[7] K. Wang, M. Wu, and S. Shen, “Secure trust-based cooperative communications in wireless multi-hop networks,” in Communications and Networking J. Peng, Ed., Rijeka, Croatia: Intec, Sep. 2010 Ch. 18, pp. 360–378,.

[8] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao, “Sybil Limit: A near optimal social network defense against Sybil attack,” IEEE/ACM Trans. Netw., vol. 18, no. 3, pp. 3–17, Jun. 2010.

[9] H. Yu, M. Kaminsky, P.B. Gibbons, and A. Flaxman, “Sybil Guard: Defending against Sybil attack via social networks,” IEEE/ACM Trans. Netw., vol. 16, no. 3, pp. 576–589, Jun. 2008.

[10] A. Tversky, “Features of similarity,” Psychological Rev., vol. 84, no. 2, pp. 327–352, 1977.

[11] F. Musau, G. Wang, and M. B. Abdullah, “Group formation with neighbor similarity trust in P2P e-commerce,” in Proc. IEEE Joint Conf. Trust, Security Privacy Compute. Common. Nov. 2011, pp. 835–840.

[12] G. Danezis and P. Mittal, “Sybil Infer: Detecting Sybil attack peers using social networks,” in Proc. Netw. Distrib. Syst. Security Symp. San Diego, CA, USA, Feb. 2009, pp. 1–15.

[13] J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil attack in sensor networks: Analysis and defenses,” in Proc. 3rd Int. Symp. Inf. Process. Sensor Netw. Apr. 2004, pp. 1–10.

[14] W. Wei, X. Feng Yuan, C. T. Chiu, and L. Qun, “Sybil Defender: Defend against Sybil attacks in large social networks,” in Proc. IEEE Int. Conf. Compute. Common. 2012, pp. 1951–1959.

[15] L. Xu, S. Chain an, H. Takizawa, and H. Kobayashi, “Resisting Sybil attack by social network and network clustering,” in Proc. Int. Symp. Appl., 2010, pp. 15–21.

[16] N. Tran, B. Min, J. Li, and L. Subramanian, “Sybil-resilient online content voting,” in Proc. 6th USENIX Symp. Netw. Syst. Des. Implementation, 2009, pp. 15–28.

[17] I. Stoica, R. Morris, D. Karger, F. Kaashoek, and H. Balakrishnan, “Chord: A scalable peer-to-peer lookup service for internet applications,” in Proc. Conf. Appl., Technol., Archit., Protocols Compute. Common, 2001, pp. 149–160.

[18] B.S. Jyothi and D. Janakiram, “SyMon: A practical approach to defend large structured P2P systems against Sybil attack,” Peer-to-Peer Netw. Appl., vol. 4, pp. 289–308, 2011.

[19] E. Damiani, D. C. Di Vimercati, S. Paraboschi, P. Samarati, and F. Violante, “A reputation-based approach for choosing reliable resources in peer-to-peer networks,” in Proc. 9th ACM Conf. Compute. Common. Security, 2002, pp. 207–216.

[20] L. V. Ahn, M. Blum, N. J. Hopper, and J. Langford, “CAPTCHA: Using hard AI problems for security,” in Proc. 22nd Int. Conf. Theory Appl. Cryptographic Tech, 2003, pp. 294–311.

[21] A. Ramachandran and N. Feaster, “Understanding the network level behavior of spammers,” in Proc. Conf. Appl., Technol., Archit., Protocols Compute. Common. 2006, pp. 291–302.