RESEARCH ARTICLE OPEN ACCESS

Secure Level Alien Parallel Trust against Sybil Attack in P2P E-Commerce

Desamuthu Pushpalatha [1], Veguru Gayathri [2], Yeturu Jahnavi [3]
PG Scholar [1], Associate Professor [2], Professor [3]
Department of Computer Science and Engineering
GIST, Nellore
AP - India

ABSTRACT

Peer to peer (P2P) e-commerce applications exist at the edge of the Internet with vulnerabilities to passive and active attacks. These attacks have pushed away potential business firms and individuals whose aim is to get the best benefit in e-commerce with minimal losses. The attacks occur during interactions between the trading peers as a transaction takes place. Sybil attack is addressed as an active attack, in which peers can have bogus and multiple identities to fake their own. Most existing work, which concentrates on social networks and trusted certification, has not been able to prevent Sybil attack peers from doing transactions. Neighbor similarity trust relationship is used to address Sybil attack. Duplicated Sybil attack peers can be identified as the neighbor peers become acquainted and hence more trusted to each other.

Keywords:- P2P

I. INTRODUCTION

P2P networks range from communication systems like email and instant messaging to collaborative content rating, recommendation, and delivery systems such as YouTube, Gnutela, Facebook, Digg, and BitTorrent. They allow any user to join the system easily at the expense of 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. Each peer plays the dual role of 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.

II. RELATED PROBLEM

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. The number of identities that an attacker can generate depends on the attacker's resources such as bandwidth, memory, and computational power. The goal of trust systems is to ensure that honest peers are accurately identified as trustworthy and Sybil peers as untrustworthy.

Defending against Sybil attack is quite a challenging task. 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. This must be counter 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.

SYBIL ATTACK OVERVIEW

A peer can give positive recommendation 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.

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. These Sybil are used to launch security attacks, both at the application level and at the overlay level. At the application level, Sybil can target other honest peers while transacting with them, whereas at the overlay level, Sybil 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 rely on a trusted central authority to prevent maliciousness.

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. Authentication-based mechanisms are used to verify the identities of the peers using shared encryption keys, or location information.

Social network is used to eliminate Sybil attack, and the findings are based on preventing Sybil identities.

III. LITERATURE SUMMARY

Experience with an object reputation system for peer to peer file sharing

Credence, a decentralized object reputation and ranking system for large-scale peer-to-peer file sharing networks. Credence counteracts pollution in these networks by allowing honest peers to assess the authenticity of online content through secure tabulation and management of endorsements from other peers. Our system enables peers to learn relationships even in the absence of direct observations or interactions through a novel, flow-based trust computation to discover trustworthy peers. We have deployed Credence as an overlay on top of the Gnutella file sharing network, with more than 10,000 downloads of our client software to date. We describe the system design, our experience with its deployment, and results from a long-term study of the trust network built by users. Data from the live deployment shows that Credence's flow-based trust computation enables users to avoid undesirable content. Honest Credence clients can identify three quarters of the decoys encountered when querying the Gnutella network.

Footprint: Detecting Sybil attacks in urban vehicular networks

In urban vehicular networks, where privacy, especially the location privacy of anonymous vehicles is highly concerned, anonymous verification of vehicles is indispensable. Consequently, an attacker who succeeds in forging multiple hostile identifies can easily launch a Sybil attack, gaining a disproportionately large influence. In this paper, we propose a novel Sybil attack detection mechanism, Footprint, using the trajectories of vehicles for identification while still preserving their location privacy. More specifically, when a vehicle approaches a road-side unit (RSU), it actively demands an authorized message from the RSU as the proof of the appearance time at this RSU. We design a location-hidden authorized message generation scheme for two objectives: first, RSU signatures on messages are signer ambiguous so that the RSU location information is concealed from the resulted authorized message; second, two authorized messages signed by the same RSU within the same given period of time (temporarily linkable) are recognizable so that they can be used for identification. With the temporal limitation on the link ability of two authorized messages, authorized messages used for long-term identification are prohibited. With this scheme, vehicles can generate a location-hidden trajectory for location-privacy-preserved identification by collecting a consecutive series of authorized messages. Utilizing social relationship among trajectories according to the similarity definition of two trajectories, Footprint can recognize and therefore dismiss "communities" of Sybil trajectories. Rigorous security analysis and extensive trace-driven simulations demonstrate the efficacy of Footprint.

Detecting Sybil attacks in VANETs

Sybil attacks have been regarded as a serious security threat to Ad hoc Networks and Sensor Networks. They may also impair the potential applications in Vehicular Ad hoc Networks (VANETs) by creating an illusion of traffic congestion. In this paper, we make various attempts to explore the feasibility of detecting Sybil attacks by analyzing signal strength distribution. First, we propose a cooperative method to verify the positions of potential Sybil nodes. We use a Random Sample Consensus (RANSAC)-based

algorithm to make this cooperative method more robust against outlier data fabricated by Sybil nodes. However, several inherent drawbacks of this cooperative method prompt us to explore additional approaches. We introduce a statistical method and design a system which is able to verify where a vehicle comes from. The system is termed the Presence Evidence System (PES). With PES, we are able to enhance the detection accuracy using statistical analysis over an observation period. Finally, based on realistic US maps and traffic models, we conducted simulations to evaluate the feasibility and efficiency of our methods. Our scheme proves to be an economical approach to suppressing Sybil attacks without extra support from specific positioning hardware.

Optimal Sybil-resilient peer admission control

Peer-to-peer and other decentralized, distributed systems are known to be particularly vulnerable to Sybil attacks. In a Sybil attack, a malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system. By controlling a large fraction of the nodes in the system, the malicious user is able to ―out vote the honest users in collaborative tasks such as Byzantine failure defenses. This paper presents Sybil Guard, a novel protocol for limiting the corruptive influences of Sybil attacks. Our protocol is based on the ―social network among user identities, where an edge between two identities indicates a human-established trust relationship. Malicious users can create many identities but few trust relationships. Thus, there is a disproportionately-small ―cut in the graph between the Sybil nodes and the honest nodes. Sybil Guard exploits this property to bound the number of identities a malicious user can create. We show the effectiveness of Sybil Guard both analytically and experimentally.

IV. PROBLEM ANALYSIS

Neighbor similarity trust is used in a group P2P ecommerce based on interest relationships, to eliminate maliciousness among the peers. This is referred 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.

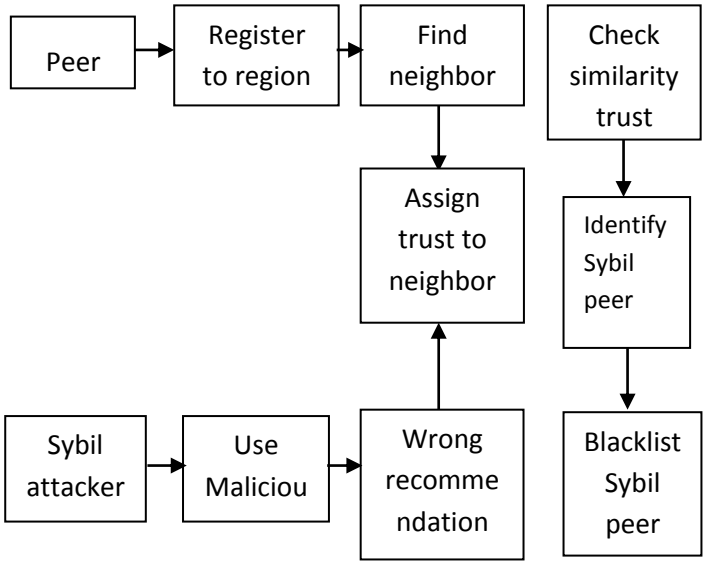
Peers use self-certifying identifiers that are exchanged when they initially come into contact. These can be used as public keys to verify digital signatures on the messages sent by their neighbors.

More honest peers are admitted compared to malicious peers, where the trust association is aimed at positive results.

Distributed admission control is used which only requires each peer to be initially aware of only its immediate trusted neighbors, and to look for honest neighbors. The neighbors assist to locate other peers of same interest in other levels.

Sybil Trust can identify and protect honest peers from Sybil attack. The Sybil peers can have their trust canceled and dismissed from a group.

V. SYSTEM ARCHITECTURE



Based on the group infrastructure in P2P e-commerce, each neighbor is connected to the peers by the success of the transactions it makes or the trust evaluation level. A peer can only be recognized as a neighbor depending on whether or not trust level is sustained over a threshold value.

Sybil Trust enables neighbor peers to carry recommendation identifiers among the peers in a group. Group detection algorithms to identify Sybil attack peers to be efficient and scalable in large P2P e-commerce networks.

VI. IMPLEMENTATION

Peer registration

Peer register with a location details. Each peer in a P2P network is given a unique identity. 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 use of social networks between two peers represents real-world trust relationship between users.

Find neighbor peer

Each peer can identify its neighbors based on peer location. We assume location to be split into groups, for example, 100, 200 etc are assigned as peer location. peer which is between 0 to 100 comes as its neighbor peers and peer between 101 to 200 becomes the next group to cooperate.

Assign trust to neighbor

Each peer in a group can assign trust value to its neighbor peer in a group. Trust value like 0 or 1, which represents normal peer or attack peer. The neighborhood of a peer v in a P2P e-commerce is N(v)={z/(v,z)ЄE}. Each peer v maintains a set of identifiers of its neighbors N(v); in which each one is unique.

Sybil attacker

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.

Sybil attack identification

If the peer trades with very few unsuccessful transactions, we can deduce the peer is a Sybil peer. A peer u and a Sybil peer v can trade whether one is Sybil or not. Being in a group, comparison can be done to determine the number of peers which trade with peer.

VII. CONCLUSION

Sybil Trust, a defense against Sybil attack in P2P e-commerce is proposed. Compared to other approaches, this approach is based on neighborhood similarity trust in a group P2P e-commerce community. This approach exploits the relationship between peers in a neighborhood setting. The results on real-world P2P e-commerce confirmed fast mixing property hence validated the fundamental assumption behind Sybil Guard's approach. Also describe defense types such as key validation, distribution, and position verification. This method can be done at in simultaneously with neighbor similarity trust which gives better defense mechanism. For the future work, intend to implement Sybil Trust within the context of peers which exist in many groups. Neighbor similarity trust helps to weed out the Sybil peers and isolate maliciousness to specific Sybil peer groups rather than allow attack in honest groups with all honest peers.

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. Comput. Commun., 2011, pp. 1–9.

[3] K. Walsh and E. G. Sirer, "Experience with an object reputation system for peer to peer filesharing," 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. Comput., 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. Comput. Commun., 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: InTech, Sep. 2010 ch. 18, pp. 360–378,.

[8] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao, "SybilLimit: A nearoptimal 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, "SybilGuard: 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.