Sybil Attacks in P2P Networks: A Survey

Ms. Dhivyabharathi S[1] Mrs. Roopachandrika R[2] Dr. Karthik S[3]
[1]P.G. Student [2]Associate Professor [2]Dean
[1,2,3]Department of Computer Science Engineering
[1,2,3]SNS College of Technology, Coimbatore

Abstract— *The Peer-to-peer Domain is that they are continuously exposed to Sybil attacks un-authenticate nods can adjust the network by implementing and developing huge amount of imaginary integrities. Now In this survey paper Focused the work for internet security related issue in the Peer to Peer Network. This survey paper include the some Security Related Information over the internet .various issue in the security for the E-commerce, Introduction part of its application and some of the security issue in the social networks . In this article, different types of Sybil attacks, comprising those arising in peer to peer prominence systems, automatic-establishing networks and social network systems are discussed. Also, many techniques are recommended more sessions to reduce or avoid their liability thoroughly are also evaluates.*

Keywords— Sybil Attack, Peer To Peer Networks

I. INTRODUCTION

P2P domain is a best route for constructing sharing applications such that the single nodes have balanced aspect. Peer to peer is also called a task organization. P2P is different domain systems to that contribute by universal patron design. P2P domain have no any hierarchy therefore no administrator is responsible for the network.P2P overlay networks are recognized for their various craved characteristic namely broad-mindedness, ambiguity, scatteraized, automatic-establishment, extensibility, and defect resilience. P2P networks and further research, freeriding is found to normal endure in the live peer to peer domain network, and then the authenticate problems about whitewashing and Sybil -resilient.

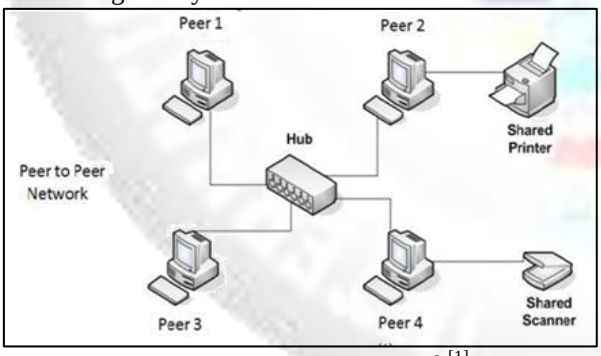

Fig. 1: Peer To Peer Network[1]

A. Sybil attack

A Sybil attack is one in which an attacker creates and control more than one identity on a single device. If a structure on a domain does not know about another domain structures, it will recognize them purely as informational introduction namely integrities. This aggression comes when the one-to-one correspondence between an entity and its identity is violated. They affect a number of application domains and environments in a variety of ways. For instance, the prominence model of peer to peer domain system may be adjustable as the aggression is able to favorably alter prominence achieves by the use of the recently developed cheater authentication.

B. Cyber Attacks

In the past, India used to be a target of cyber aggression for constitutional desire only. Some previous and now a days, the global cybercrime landscape has changed dramatically, with culprits working most matured techniques and huge intelligence of computerized preservations. Until recently, malware, inbox mails, thefting into company URLS and more aggression of this nature were mostly the work of computer 'geniuses' proves their intelligence. These intrusion, which were strangely malevolent, have gradually derived into computerized culprits association convey outside currency over prohibited computerized networks.

In this survey on recent schemes which focus on detect and avoid Sybil attacks in p2p system is provided. This study can define the sybil-resilient transfer peer to peer techniques and a charismatic prominence technique. Merging more techniques to detect and prevent Sybil attacks in peer to peer networks systems are discussed. We are focus on p2p networks for E-commerce system attacks. This problem solving to proposed a Sybil framework to controlling nodes to getting more process units in a sensible steps and find the destructive across Sybil attack.

II. TYPES OF SYBIL ATTACKS

A. Data Aggregation

Sensor network readings are computed by query protocols in a network rather than returning the observing of all single sensors. This is achieving to consume efficiency. Sybil identities may be able to report incorrect sensor observing thereby affecting the moreover find outs combined. A malicious user may be able to significantly alter the aggregate with enough identities.

B. Fair Resource Allocation

Sybil attacks enable the attacker to obtain not well and improper huge transfer of ability that were originally intended to be distributed amongst all nodes on the network equally. This attack repudiates legitimate nodes their deserved share of resources and provides the malicious node with more avenues for other attacks.

C. Routing

Sybil attacks can distort routing protocols in ad hoc networks, importantly the many path tracking technique. Individual routes that initially seem disjoint may pass through the Sybil nodes of a each one malicious. More than one hard topic is Geographical routing where malicious nodes may appear in more than one place at a time.

D. Distributed Storage

File storage systems in peer-to-peer and wireless sensor networks can be adjustable by the network malicious. This

is done by defeating the fragmentation and replication processes in the data service. A method can be frauded into saving data into the multiple Sybil identities of the same node on the network.

E. Tampering with Majority and Prominence Method

In any network system where there is a voting method in position for uses such as explain and detecting node malicious in the system, updating reputation scores and so on, a network malicious may be significantly terrible. As an example, an attacker may create enough malicious identities to continuously addressed and ensure revocate consistence nodes from the network.

III. TECHNIQUES SCHEDULED TO SYBIL ATTACKS

Some techniques mitigate the threat level of these attacks in a system to a satisfactory minimum without incurring an appreciable performance overhead. Although they will not completely eliminate the possibility of the attack occurring, they are more than worthy of consideration.

A. Keep Your Friends Close

In this section, First, motivated by the observed relationship between the quality of the algorithmic property and hypothesized trust in social graphs, we propose several designs, each in the form of modified random walk, to model trust in social networks. Second, we learn the impact of the different designs on the performance of the Sybil defenses by comparing them to each other when operated on top of Syil Limit, a method for opposed across the network malicious using social networks.

B. Footprint Based Detection

In Footprint, implement a position-mysterious identities information reported scheme for two purposes. First, RSU signatures on messages are user-anonymous which means an RSU is unauthenticated when checking a message. In this way, the RSU location information is depended from the last secured information. Next, secured information's are temporarily linkable which means two authorized information shared from the same RSU are acceptable if and only if they are issued within the same period of time.

C. Random Sample Consensus (RANSAC)-based Detection

Study the feasibility of using signal strength distribution analysis to find network malicious. startly, we build a unit based finding system, in which multiple neighboring nodes cooperate to compute the waves energy dissemination of a significant node and verify the physical position of the suspicious node. We use a RANSAC method technique to increase the estimation robustness against outlier data fabricated by Sybil nodes. The concept of Presence Evidence System (PES). With this system, we can ensure that nodes in the defending congestion are real nodes and we can have them as the trusty sources of signal strength measurements.

D. Gatekeeper - Sybilresilient Admission Control Protocol

Here, present a distributed Sybil-resilient admission control protocol called Gatekeeper. Given a social network G which exposed a arbitrary expander-graph feasibility, This process achieves the bellow process with more feasibility:

1) In the face of k attack edges with k up to O(n/ log n), Gatekeeper limits the number of admitted Sybil identities to be O(log k) per malicious node. This explains that only O(1) attacker nodes are conformed each malicious corner if the malicious has O(1) malicious rate.
2) Gatekeeper admits almost all honest users.

E. SybilLimit Protocol

Present a new protocol that leverages the unique technique as SybilGuard but outside badly increased and perfect security. We use the technique SybilLimit, because i) it curb the many of attacker nodes adjusted and ii) it is perfect and thus complete the method to the deadline.

F. SybilGuard Protocol

SybilGuard, a novel decentralized technique that controls the forging impact of network malicious, including sybil attacks exploiting IP harvesting and even few malicious introduced from botnets off the method. Our design is based on a unique insight regarding social network where identities are nodes in the graph and edges are human-established trust relations. The edges connecting the honest region and the sybil region are called attack edges.

G. Group Formation with Neighbor Similarity Trust

We now unit construction of peers established on the involvement to sharing in an e-commerce domain. Peers, which have normal nearby nodes form a same as cluster among the nearby nodes, which contributes to minimize maliciousness. We present a simple process to find for items established on same as involvement, as each group shares the type of products or methods it processed.

H. Sybil Attack - Analysis & Defenses

We analyze how an attacker can use the different types of the Sybil malicious to annoy or adjustable various sensor domain system techniques. We propose several new defenses against the Sybil attack, combined waves ability finding, authenticate checked for arbitrary authentication pre-dissemination, location checking, and conformation. Through quantitative analysis, we show that the radio resource checking process is more energetic build the expectations that a malicious node cannot send on multiple channels simultaneously. We also present a quantitative evaluation for the arbitrary authentication dissemination method appearing that it is terrific to adjustable nodes.

I. SybilDefender Protocol

Established on processing a curbed compute of arbitrary transmission within the network research, the attack authentication technique and the attack region checking methods are effective and flexible to huge social networks. We evaluate SybilDefender using more than one huge applications samples from Whatsapp and Facebook, respectively. And it outperforms SybilLimit, the overall results of attack security techniques that used to huge domains, by one to two orders of magnitude in both accuracy and running time. Here propose two practical techniques to limit the number of attack edges in online domains, and implement a Facebook processor to detect the property of one of the methods.

J. Sybil Resisting Network Clustering (SRNC)

In SRNC, an bountry is accepted a probable malicious bountry if its betweenness is high. This is reason of all the minimom cost routes between original users and Sybil peers have to traverse attack edges. Therefore, SRNC first computes the betweenness of each edge and identifies the edges with extremely high betweennesses. Then, SRNC inhibits the communication via the identified edges. Finally, the performance of SRNC is evaluated by both theoretical checking and practical exposing file groups of original world community domain.

K. Chord - Distributed Lookup Protocol

The Chord method, the percentage of its originality, and practical results demonstrating the strength of the algorithm. We also address few common conclusion on working the Chord path technique can be extended to take into account the physical domain region. Followers involved in an process of Chord and how Chord behaves on a small Internet tested are referred to Dabek.

L. SyMon Protocol

In our sybil defense scheme, every peer isassociated with another peer, known as SyMon (SybilMonitor). The SyMon of any mentioned user is selecting forcefull like that the originality of both of them being sybils is very low. The chosen SyMonprevents the mentioned attack from focusing another original user by checking the transactions involving the given peer.

M. Reputation-Based Approach

Here, present a protocol, called XRep, for maintaining and exchanging reputations that can be honestly boosted on previous peer to peer techniques, and discuss the advantages it provides against known attacks to peer to peer domains. We review the equivalent pros and cons of resource-based vs. servant-based reputation results and therefore how their composed use can solution pros. It is important to note that, while it can be easily.

N. CAPTCHA Security

We introduce captcha, a self check that man can share, but now cyber techniques can't pass: any program that has high success over a captcha can be expose to finish an unfinished AI trouble. We give various robust implements of trust. Now also captchas have more processes in real time authentication, Here a method abstraction a current level of most troubles that can be exploited for security purposes.

O. IDMaps Framework

In this framework, we propose a global architecture for online publish radius assumption and dissemination which we request IDMaps. We used to have IDMaps be the underlying service that gives the orbit messages used by SONAR/HOPS. We argue the basic IDMaps architecture and show, through Internet experiments and practical, that our method can naturally give meaningful orbit messages.

P. DSybil Approach

Here, will use the session attack integrities to mention to all selfish/ adjustable/ defect/ attack integrities. Defending against sybil identities is normally silent objection, and the indeed of reference methods makes it even harder.

Q. EigenTrust Algorithm

Here, trying to authenticate attack users that provide in authentic files is superior to attempting to check anonumy data in self-organizing, since attacker users can easily generate a virtually unlimited number of anonumy data if they are not avoided from used in the network. We present such a method wherein each peer i is an accepted a peculiar universal original rate that rereact the experiences of all peers in the network with peer i. This method, whole peers in the domain perform in calculating these rates in a dissemination and node-symmetric manner with minimal overhead on the network.

R. Trust Management with Delegation

This algorithm is based on Eigen Trust where a user will compute universe original rate by getting prominence rates from all peers in network. Eigen Trust does not take into login person efficient, nor does it taken the energy of resource. We propose a model called Eigen Group Trust which carries mant of the disadvantages of this process. Here also propose a delegation model that can not only be extended to cluster establishment P2P region but can also give an powerful resource measure.

S. Received Signal Strength Indication (RSSI)

A new method of Sybil attack detection in WSN based on received signal strength. First, the new method establishes a practical network space channel model of WSN between nodes, which accords with Rayleigh fading process. Secondly, the new method judges the Sybil attack synthetically according to the received signal strength, such as ID, position, power value, received signal strength. Third, aiming at the Sybil attack of head nodes and member nodes, the new method designed two detection ways to improve the efficiency and refinement.

T. Measurement& Analysis-Online Social Networks

Here, present a huge computational journal and checking of the design of four recent internet commnual domains: Twitter, Facebook, and Whatsapp. Data gathered from multiple sites enables us to identify equal designed feasibility of internet communal domains. We believe that ours is the first study to examine multiple online social networks at scale

IV. CONCLUSION

Many P2P domain techniques are very hard to internet communal domain attacks. The Sybil attack is an attack where in a reputation system is corrupted by a acceptable many of fraud authentities in peer-to-peer networks. In this paper, important types of more aggression that can be mentioned on many processes regions are argued. Methods that have been proposed over time to tackle these attacks are also listed.

REFERENCES

[1] A. Mohaisen, N. Hopper, and Y. Kim, "Keep your friends close:Incorporating trust into social network-

based Sybil defenses," inProc. IEEE Int. Conf. Comput. Commun., 2011, pp. 1–9.

[2] 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.

[3] 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.

[4] T. Nguyen, L. Jinyang, S. Lakshminarayanan, and S. M. Chow,"Optimal Sybil-resilient peer admission control," inProc. IEEEInt. Conf. Comput. Commun., 2011, pp. 3218–3226.

[5] H. Yu, P. Gibbons, M. Kaminsky, and F. Xiao, "SybilLimit: A nearoptimal social network defense against Sybil attack,"IEEE/ACMTrans. Netw., vol. 18, no. 3, pp. 3–17, Jun. 2010.

[6] H. Yu, M. Kaminsky, P.B. Gibbons, and A. Flaxman, "SybilGuard:Defending against Sybil attack via social networks,"IEEE/ACMTrans. Netw., vol. 16, no. 3, pp. 576–589, Jun. 2008.

[7] F. Musau, G. Wang, and M. B. Abdullahi, "Group formationwith neighbor similarity trust in P2P e-commerce," inProc.IEEE Joint Conf. Trust, Security Privacy Comput. Commun., Nov.2011, pp. 835–840.

[8] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack insensor networks: Analysis and defenses," inProc. 3rd Int. Symp.Inf. Process. Sensor Netw., Apr. 2004, pp. 1–10.

[9] W. Wei, X. Fengyuan, C. T. Chiu, and L. Qun, "SybilDefender: Defend against Sybil attacks in large social networks," inProc. IEEE Int. Conf. Comput. Commun., 2012, pp. 1951–1959.

[10] L. Xu, S. Chainan, H. Takizawa, and H. Kobayashi, "Resisting Sybil attack by social network and network clustering," inProc. Int. Symp. Appl., 2010, pp. 15–21.

[11] I. Stoica, R. Morris, D. Karger, F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," inProc. Conf. Appl., Technol., Archit., Protocols Comput. Commun, 2001, pp. 149–160.

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

[13] 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," inProc. 9th ACM Conf. Comput. Commun. Security, 2002, pp. 207–216.

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

[15] P. Francis, S. Jamin, C. Jin, Y. Jin, D. Raz, Y. Shavitt, and L. Zhang, "IDMaps: A global internet host distance estimation service," IEEE/ACM Trans. Netw., vol. 9, no. 5, pp. 525–540, Oct. 2001.

[16] H. Yu, C. Shi, M. Kaminsky, P. B. Gibbons, and F. Xiao, "DSybil: Optimal Sybil-resistance for recommendation systems," inProc. IEEE Symp. Security Privacy, 2009, pp. 283–298.

[17] S. D. Kamvar, M. T. Scholosser, and H. G. Molina, "The EigenTrust algorithm for reputation management in P2P networks," in Proc. 12th Int. World Wide Web, May 2003, pp. 640–651.

[18] A. Ravichandran and J. Yoon, "Trust management with delegation in grouped peer-to-peer communities," in Proc. ACM Symp. Access Control Models Technol., 2006, pp. 71–80.

[19] J. Wang, G. Yang, Y. Sun, and S. Chen, "Sybil attack detection based on RSSI for wireless sensor network," inProc. IEEE on Wireless Commun., Netw. and Mobile Comput. Sep. 2007, pp. 2684–2687.

[20] A. Mislove, M. Marcon, K. P Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and analysis of online social network," in Proc. 7th ACM SIGCOMM Conf. Internet Meas, 2007, pp. 29–52.