ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Efficient Sybil Attack Defence Mechanisms in Large Social Networks

Piyush Chandekar, Dr. Shalu Chopra

PG Student, Dept. of I.T., VESIT College, Mumbai University, Maharashtra, India

Head of Department, Dept. of I.T., VESIT College, Mumbai University, Maharashtra, India

ABSTRACT: Sybil attack on a large social network analyzed by different defending techniques. Sybil attack has become an alarming threat for open access decentralized systems that allows an attacker to take unfair advantage of system resources and manipulate the network behavior. To defeat such harmful tool, several protective techniques have been proposed. The comparison of previously proposed defense algorithms based on their assumptions, features and various other parameters is done. Important inferences for existing Sybil defense schemes as well as their future designs have also been considered.

KEYWORDS: Sybil attacks, Sybil nodes, distributed systems, trusted certification, resource testing, random walks

I. INTRODUCTION

The fully decentralized peer-to-peer networks are mostly susceptible to Sybil attack. Under Sybil attack the malicious attacker also known as Sybil node generates multiple fake identities. Through these identities attacker makes an illusion that these are different peers in a network. The upper limit to create fake identities depends completely on the potential of an attacker. Hence, the collaborative decisions of honest nodes can be influenced when large number of Sybil node present in a system sends erroneous decisions.

To address such attacks many defending schemes were developed. The goal of these defence systems is to identify Sybil nodes and prohibit them to exploit the network resources. Based on the functionality, the defensive schemes have been categorized in two broad categories, as- 1) trusted certification and 2) resource testing. Trusted certification based testing is further subdivided into- centralized certification authority (CCA), decentralized cryptographic primitives (DC) and trusted device (TD). Similarly, resource testing is sub-classified as - internet protocol testing (IPT), cost recurrence (CR) and testing through social graphs. Protocols falling under first group possess some certificates, verification stream or keys so that legitimate nodes can be identified in a network [1]. Resource testing includes the testing of available resources like IP address and then finding out the geographical area of the user. If multiple entries are received from the same region then those identities will be marked as an attacker.

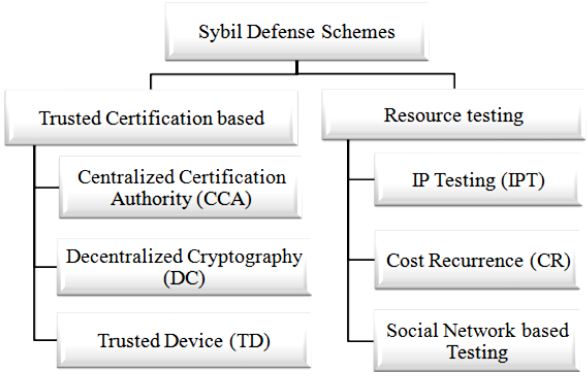

Fig.1.Classification of Sybil defence schemes based on the function and type of testing

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

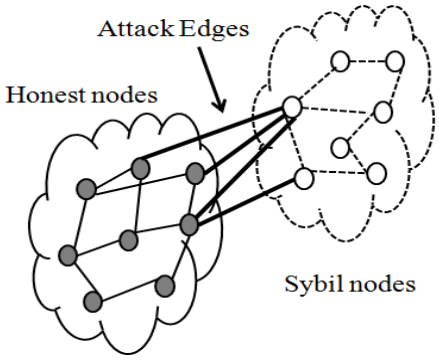

Fig.2. Honest nodes, Sybil nodes and their attack edges in a network

Cost recurrence procedure asks users to solve puzzles or some testes like CAPTCHA, or add their phone numbers to distinguish between authorized nodes and fake nodes. This work focuses on the third sub-type of resource testing i.e. social network based Sybil defense system. It is a scheme that utilizes the trust of social links to identify honest nodes. Hence, this method is more efficient and effective to discover Sybil nodes. Detailed classification is shown in figure 1.

The paper aims to examine, the existing defending mechanisms for Sybil attack, in large social networks. Description of other type of schemes have not been included in this work, only the methods that are built upon social graphs or networks are considered for comparison and included in sub-sequent sections. In [3], [4], [5], [6] and [8] defending mechanisms have been introduced. These are SybilDefender, SybilGuard, sublimit, SybilInfer and SumUp respectively. In [2], previously, most of these mechanisms have been compared. We are following the same comparison table with little addition.

The rest of the paper is as follows. Section 2 briefs the considered defending schemes SybilDefender, SybilGuard, sublimit, SybilInfer and SumUp, for the analysis. Section 3 represents the comparison of these algorithms and the paper concludes with section 4.

II. LITERATURE SURVEY

The network is a combination of Sybil and non-Sybil regions. In such network to discover malicious nodes the assumption is made, that, even if an attacker creates numerous identities in a social network, it won't be able to set up massive social links with legitimate nodes. Thus, it is weakly connected to the rest of the network but can connect to other Sybils. The links between the honest node and Sybil is named as 'attack edges' and the two regions are separated by 'small cut', shown in figure 2. The social graph created through these links is verified to spot out Sybils [2]. All the algorithms are based on the random walks i.e. sequence of moves between nodes in a network.

The brief introduction of some schemes is given in the following sub-sections.

2.1. *SybilDefender*:

The recently designed mechanism SybilDefender is a centralized scheme, composed of three phases- Sybil identification, Sybil community detection and two schemes to restrict the number of attack edges [3]. Sybil identification algorithm executes in two steps and find outs the Sybil node through random walk approach. Random walks of honest nodes are longer than that of Sybil nodes. Once the Sybil node is trapped Sybil community algorithm detects neighboring Sybil nodes. Hence, in this mechanism there is no need to examine each node to find Sybil region as in SybilGuard and SybilLimit algorithm. The partial random walk (where a node does not traverse the intermediate node more than a time) so performed will not leave the Sybil region, thus, it will be die-out within that region only. Hence detection of Sybil region through this separate algorithm reduces the time consumed n examine each node. Relationship rating and activity network are two approaches to limit the number of attack edges. In relationship rating members of social network rate their relationships. Activity network is a graph that is designed on the basis of interaction between users. This scheme is comparably more accurate and faster [3].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

2.2. *SybilGuard*:

This is a decentralized scheme, assumes that the social network has property of fast mixing. Where, only honest node regions support this property. Here, single Sybil is detected at a time, thus, to find complete group all the nodes need to be examined [4]. The SybilGuard mechanism uses a special type of random walks, known as random routes, where, each node follows a randomized routing table for the selection of next hop. If the random walk from honest node and a given node intersects, SybilGuard considers that node as benign or honest otherwise it is treated as an attacker. The main drawback of this algorithm is that, it works only on a fast mixing network; in a slow mixing network honest node can be marked as an attacker, by mistake. Moreover, it is less efficient in terms of reliability because many Sybils still exist in a network.

2.3. *SybilLimit*:

The action of SybilLimit protocol is based on the same assumption as SybilGuard, but its modified features enhance the reliability of scheme. This decentralized protocol identifies one Sybil at a time, similar to SybilGuard with some modification. Where SybilGuard accepts $O(\sqrt{n}\log n)$ Sybil nodes / attack edge (n- number of honest nodes), SybilLimit accepts O(log n) Sybil nodes / attack edge. To find out the Sybil community SybilLimit performs random walks from each node. Random walks start from an honest node. Based on the results of two conditions- intersection and balanced conditions, an honest node decides whether the given node is Sybil or not. The intersection condition says that, the last edge of one of the random walks of an honest node and the given suspect is required to intersect, to declare it non-Sybil. In case of balance condition each accepted node increases 'load' of some tails that should not result in a long "load spike" and cause to exceed a given threshold. The load is incremented when the verifier node marks a suspect as a non-Sybil. This balance condition was not adopted in SybilGuard [5]. This protocol is more efficient than the SybilGuard but has

2.4. *SybilInfer*:

A probabilistic model of honest social networks, and Bayesian inference technique to mark Sybil region are the foundation of SybilInfer mechanism [6]. This centralized defense mechanism is built upon the similar assumption as SybilGuard and SybilLimit with the addition that a node is acquainted with the entire social network topology which is static in nature. This algorithm performs number of random walks from every node to section non-Sybil region. Then it uses a Bayesian inference technique for the determination of the probability of node being marked as non-Sybil [2]. Since the entire graph is not fast mixing, if a Sybil connects another Sybils to its thin attack edges, the conductance of graph as well as the Sybil area becomes smaller and hence next Sybil nodes can be found. There is no analytical bound on the acceptance of number of Sybils / attack edges [7]. This technique is shown to be more reliable than SybilGuard and SybilLimit in [6]. Besides the advantages, it has high computational overheads and can handle small network up to 30,000 nodes, which is very small as compared to the actual size of the social networks [3].

2.5. *SumUp*:

It is a centralized mechanism that addresses the vote aggregation problem in a network under the influence of Sybil identities. To get the best decision regarding the quality of online system, voting is done. In this case, to isolate the voting process from Sybils, the solution needs that – 1) all the votes from honest nodes must be accepted, 2) it 'eA' is the number of attacking edges from an attacker then its fake voting should restricted to 'eA' only, and 3) if Sybil continuously sends forged vote, it should be boycotted in the future [8]. An adaptive vote flow aggregation technique of this protocol limits the number of fake votes from an attacker. SumUp aggregates opinions of honest source by calculating a set of max-flow links on the trust graph from the source to all voters. The number of forged votes is restricted by the number of attack edges in place of links among Sybil nodes because only opinions on paths with non-zero flows are considered. Cmax is a parameter used in this algorithm that decides the maximum number of votes accepted by the system. Through machine learning approach, SumUp can prohibit an attacker that continuously misbehaves. Another important assumption is that, the min-cut between the vote collector and honest nodes, occurs at the collector and between Sybils and honest it occurs at the attack edges. On an average, SumUp accepts O(log n)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Sybils/ attack edges. This algorithm requires knowledge of the overall system. The drawback of this technique is its high computation requirements and large run time [1].

III. COMPARISON OF DEFENCE MECHANISMS

Above mentioned four defense schemes- SybilGuard, SybilLimit, SybilInfer and SumUp have been previously compared in [2]. These schemes are designed for particular scenarios; hence for the ease of comparison, their assumption, random walks, graph partitioning algorithms etc. are examined in [2]. In this paper, we have considered the same parameters as in [2] for comparison with the addition of one more mechanism SybilDefender, shown in Table 1.

	SybilDefender	*Sublimit*	*SybilGuard*	*SybilInfer*	*SumUp*
Defense Type	Centralized	Distributed	Distributed	Centralized	Centralized
Assumption	Non-Sybil region is fast mixing	Non-Sybil region is fast mixing	Non-Sybil region is fast mixing	Non-Sybil region is fast mixing, modified walks are fast mixing	Non-Sybil region is fast mixing, no small cut between collector and non-Sybil region
Algorithm	Limited (partial) random walk performed by node	Multiple random walks performed by each node	Random walk performed by each node	Bayesian inference on the results of the random walks	Creation of voting envelop with appropriate link capacities around collector
Ranking	Varying random walk length	Varying number of random walks and walk length	Varying random walk length	Probability of node being non-Sybil from Bayesian inference	Varying the size of the voting envelop
Cut-off	Whether or not walk intersection occurs	Whether or not tails of random walks intersect	Whether or not walk intersection occurs	Threshold on the probability that a given node is non-Sybil	Whether or not nodes are within the voting envelope
Number of Sybils / attack edges	No analytical bound	O(log n)	O(√n log n)	No analytical bound	O(log n)
Evaluation	Facebook, Orkut	Friendster, Live Journal, DBLP, Kleinberg	Kleinberg network	Power-low network, Live Journal	YouTube, Flickr, Digg

Table 1. Properties and Evaluation of social network-based Sybil defence schemes (reproduced [2]).

IV. CONCLUSION

The analytical results of each protocol presented in [3], [4], [5], [6] and [8], indicated that recently developed SybilDefender technique is more efficient in terms of reliability, reduction of computation time and application in real-time large social network. This protocol tries to overcome all the limitations of the previously proposed techniques for social networks.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

REFERENCES.

1. Aziz Mohaisen and Joongheon Kim, "The Sybil Attacks and Defenses: A Survey", Smart Computing Review, vol. 3, no. 6, pp 489-480, December 2013.
2. B. Viswanath, A. Post, K. P. Gummadi, A. Mislove, ―An analysis of social network-based Sybil defenses,‖ in Proc. of ACM SIGCOMM, 2010.
3. Wei Wei, Fengyuan Xu, Chiu C. Tan, Qun Li (December 2013), "SybilDefender: A Defense Mechanism for Sybil Attacks in Large Social Networks" IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 12.
4. Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, Abraham D. Flaxman, "SybilGuard: Defending Against Sybil Attacks via Social Networks", IEEE/ACM Transactions on Networking, Vol. 16, No. 3, June 2008.
5. Haifeng Yu, Phillip B. Gibbons, Michael Kaminsky, Feng Xiao, "SybilLimit: A Near-Optimal Social Network Defense Against Sybil Attacks" IEEE/ACM Transactions on Networking, Vol. 18, No. 3, June 2010.
6. George Danezis, Prateek Mittal, "SybilInfer: Detecting Sybil Nodes using Social Networks", Proc. Network and Distributed System Security Symp. (NDSS), 2009.
7. Nguyen Tran, Jinyang Li, Lakshminarayanan Subramanian, Sherman S.M. Chow, "Optimal Sybil-resilient node admission control", IEEE INFOCOM 2011.
8. Tran N., Min B., Li J., Subramanian L, "Sybil-resilient online content voting", In NSDI'09: Proceedings of the 6th USENIX Symposium on Networked Systems Design and Implementation (2009),USENIX Association, pp. 15–28.
9. J.R. Douceur, "The Sybil Attack," Proc. Revised Papers First Int'l Workshop Peer-to-Peer Systems (IPTPS '01), 2002.

BIOGRAPHY

Piyush Chandekar is pursuing M.E (I.T) fromV.E.S. Institute of Technology, Mumbai University. He did his graduation B.E (CSE) from Nagpur University, Maharashtra. He iscurrently working on Trust based mechanism over peer to peer networks.