Using Multiple Verifiers to Detect Sybils in a Social Network Graph

Kyungbaek Kim

Department of Electronics and Computer Engineering
Chonnam National University, Gwangju, South Korea
kyungbaekkim@jnu.ac.kr

Abstract. Detecting Sybil identities is important to operate a distributed system without losing its openness property. Recently, OSN(Online Social Network) based Sybil detection methods are proposed and an individual node can determine whether other nodes are Sybil or not. However, since the probabilistic properties of the previous methods, single verifier based Sybil detection may suffer from the wide variance in the performance of detecting Sybil nodes. In this paper, multi-verifier based Sybil detection method is proposed to mitigate the variance. The proposed method selects honest verifiers from a social network graph where honest and Sybil nodes are mixed. Then, the method determines whether a node is Sybil or not by comparing the likelihood of acceptance of the node and a given threshold. Through the extensive evaluation with the real-world social network sample graph, the proposed multi-verifier based Sybil detection outperforms the single verifier based Sybil detection in both aspects of accepting honest nodes and suppressing Sybil nodes.

Keywords: Online Social Network, Sybil Detection, Trustness.

1 Introduction

In a distributed system, detecting Sybil identities is an important issue. Sybil identities are fake identities belong to a malicious identity and exploited to obtain immoral gains from the system or subvert the system. In a P2P system, many Sybil identities join the system and they can gain the control of the system to hamper the operations of the system [1]. These Sybil identities also threat the openness of distributed systems by making the resources of the systems untrustworthy. Another example can be observed in a collaborative recommendation system. Many Sybil identities recommend the fake assertion of a malicious identity, and let other identities trust the fake assertion [2,3]. These malicious activities conducted by Sybil identities are called ***Sybil attacks***.

A traditional way to defend the Sybil attack is increasing the complexity of generating identities such as CAPTCHA [4]. Another way is using a centralized authority which requires real-world identities such as social security numbers or credit card numbers. However, these approaches require expensive costs and cause another threats such as leaking the critical information of real identities to malicious identities.

James J. (Jong Hyuk) Park et al. (eds.), *Future Information Technology*,
Lecture Notes in Electrical Engineering 276,
DOI: 10.1007/978-3-642-40861-8_34, © Springer-Verlag Berlin Heidelberg 2014

Recently, OSN based Sybil detection methods have been proposed [5,6]. They use an online social network graph where the real world relationships are embedded. It is assumed that the online social network graph is composed of an honest region where honest identities reside and a Sybil region where Sybil identities reside, and these methods rely on the property that there are a limited number of cuts between an honest region and Sybil region. According to this, these methods let a single node in a graph determine whether a node is Sybil or not by using a probabilistic measure such random walks.

Generally, an individual node well determines whether a node is Sybil or not. However, since the previous methods use a probabilistic measure and the detecting process is conducted on each individual node, some nodes exhibit the misbehavior such that a node may consider many honest nodes as Sybil nodes or it may accidently accept many Sybil nodes as honest nodes. That is, there is wide variance in the performance of detecting Sybil nodes by using a single verifier. Also, this wide variation of the performance causes a new kind of threat such as focused Sybil attack to a targeted honest node.

In this paper, the Sybil detection method using multiple verifiers is proposed to eliminate this variance in the performance of detecting Sybil nodes. While previous methods focused on that each individual node works as a single verifier, the proposed method uses multiple nodes as multiple verifiers which are collaborated to determine which node is Sybil or not. In a social network graph, multiple verifiers are selected and each verifier conducts an OSN based Sybil detection method, SybilLimit [5] to determine which node is Sybil or not. Based on the results of verifiers, each node in the social network graph obtains a value of likelihood that a node is accepted by a verifier. That is, the likelihood value of a node represents the likelihood that the node is an honest (non-Sybil) node. This likelihood can be normalized into a value between 0 and 1, and it can be used for determining whether a node is Sybil or not.

In the proposed approach, there are two challenges: 1) how to choose verifiers and 2) how to set a threshold to determine whether a node is honest or not. To choose the good verifiers, a few pre-trust nodes are used to gather a set of candidate nodes and verifier nodes are randomly selected from the set. This selection method is required because honest and Sybil nodes are mixed in a social network graph, and this careful verifier selection prevents a Sybil node from being a verifier node. To find out a reasonable threshold, the extensive evaluation with a sampled real-world social network graph is conducted. According to the results of the evaluation, it is shown that using multiple verifiers with a reasonable threshold accepts most of honest nodes and prevents most of Sybil nodes from being accepted. Also, through the evaluation, it is shown that the importance of choosing good verifiers to guarantee the performance of detecting Sybil node by using multiple verifiers.

2 Multi-verifier Based Sybil Detection

2.1 Background and Assumption

A social network graph, $G = (V, E)$, where $|V| = N, V = \{v_1, v_2, \ldots, v_n\}$ and $|E| = M$, $e_{ij} \in E = v_i \rightarrow v_j$, can be viewed as a single strongly connected component. Each v_i is a node corresponding to an identity. If a node is corresponding to an honest identity, it is called as an honest node. Otherwise, the node is called as a Sybil node. In a social network graph, an honest (non-Sybil) region where honest nodes reside coexists with multiple Sybil regions where Sybil nodes reside. Inside a Sybil region, Sybil nodes are easily generated and each of them can be connected to each other as many as possible. But, there are the limited number of attack edges between the honest region and each Sybil regions [5,8].

SybilLimit[5] is an OSN-based Sybil detection method, and it is used to determine whether a node is honest or not. Basically, SybilLimit is used for a single verifier node to determine whether a suspect node is a Sybil node or not. The verifier node, v, prepares the verification set of tails, S_v,which is composed of $r\ (= \Theta(\log|V|))$ tails drawn from random routes of length $w\ (= \Theta\left(\sqrt{|E|}\right))$. The suspect node, s, also prepares the sample set of tails, S_s, which is composed of r tails drawn from random routes of length w. If there is any common tail in both of S_v and S_s, the verifier node accepts the suspect as honest nodes.

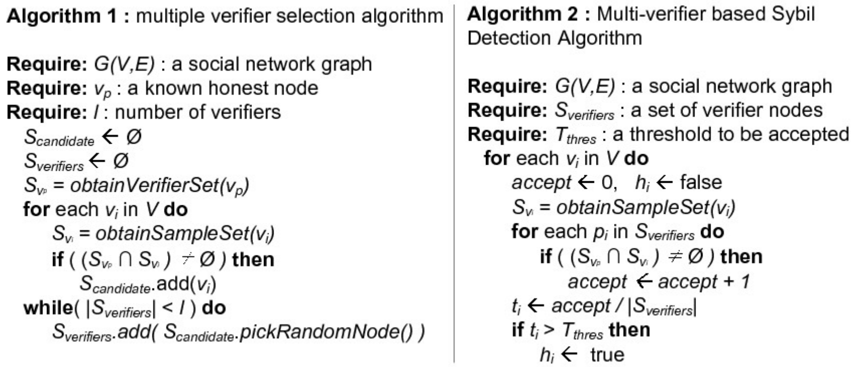
However, the performance of SybilLimit may be different from each verifier node since the process of preparing the verification set and the sample set relies on a probabilistic measure. According to this reason, some approaches have tried to use multiple verifiers and assign the Sybil-resistant trust value which indicates the likelihood that a node is honest [3,7]. But, these works still did not consider the challenges such as how to choose good verifiers and how to set a threshold to accept a node as honest.

2.2 Algorithm of Using Multiple Verifiers

The main idea of using multiple verifiers is gathering the results of detecting Sybil nodes from multiple verifiers and determining whether a node is Sybil or not based on the gathered result such as how many verifiers accept the node. To do this, a system needs a coordinator to gather/examine the results. Usually the possible coordinator can be the OSN provider which knows the entire social network graph. Also, this coordinator has a few number of trust nodes which are considered as known honest nodes.

The basic algorithm of using multiple verifiers to detect Sybil nodes is shown in Fig. 1. Algorithm 1 shows the algorithm of choosing good verifiers. At first, we use a known honest node to collect the nodes which may be honest nodes as the set of candidate verifier nodes, $S_{candidate}$. Since both honest nodes and Sybil nodes are mixed in V, during this step we need to add the nodes which is verified by the known honest node as the candidate verifier nodes. Then, l verifier nodes are randomly selected from $S_{candidate}$. According to this algorithm, we can choose honest nodes as verifier nodes to some extent and prevent that many Sybil nodes are selected as verifier nodes.

After the good verifiers are chosen by conducting Algorithm 1, multi-verifier based Sybil detection is performed like Algorithm 2. Firstly, each verifier node conducts SybilLimit based Sybil detection for a node and the likelihood value (t_i) of the node is calculated by dividing the number of verifier nodes accepting the node by the total number of verifier nodes. Then, if the likelihood value (t_i) of the node is greater than a given threshold value (T_{thres}) the node is considered as an honest node, that is, h_i becomes true.



```
Algorithm 1 : multiple verifier selection algorithm

Require: $G(V,E)$ : a social network graph
Require: $v_p$ : a known honest node
Require: $l$ : number of verifiers
  $S_{candidate} \leftarrow \emptyset$
  $S_{verifiers} \leftarrow \emptyset$
  $S_{v_p} = obtainVerifierSet(v_p)$
  for each $v_i$ in $V$ do
      $S_{v_i} = obtainSampleSet(v_i)$
      if ( $(S_{v_p} \cap S_{v_i}) \neq \emptyset$ ) then
          $S_{candidate}$.add($v_i$)
  while( $|S_{verifiers}| < l$ ) do
      $S_{verifiers}$.add( $S_{candidate}$.pickRandomNode() )
```

```
Algorithm 2 : Multi-verifier based Sybil Detection Algorithm

Require: $G(V,E)$ : a social network graph
Require: $S_{verifiers}$ : a set of verifier nodes
Require: $T_{thres}$ : a threshold to be accepted
  for each $v_i$ in $V$ do
      $accept \leftarrow 0$,   $h_i \leftarrow$ false
      $S_{v_i} = obtainSampleSet(v_i)$
      for each $p_i$ in $S_{verifiers}$ do
          if ( $(S_{v_p} \cap S_{v_i}) \neq \emptyset$ ) then
              $accept \leftarrow accept + 1$
      $t_i \leftarrow accept / |S_{verifiers}|$
      if $t_i > T_{thres}$ then
          $h_i \leftarrow$ true
```

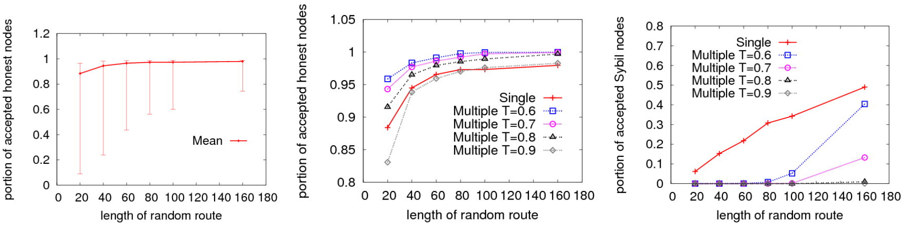
Fig. 1. Algorithms of multi-verifier based Sybil detection

3 Evaluation

To understand the limitation of single verifier based Sybil detection and evaluate the proposed multi-verifier based Sybil detection, we conducted both methods with a sample social network graph obtained from Facebook [2]. The sample graph has 50k nodes and 905,004 edges, and it is considered as an honest region. Sybil regions are generated artificially. There are 25 Sybil regions and each Sybil region has 100 Sybil nodes. A Sybil region is generated as a single strongly connected component where the average number of edges is 15, and it has 2 attack edges which are connected to honest nodes randomly.

Fig. 2(a) shows the performance of single verifier based Sybil detection, including minimum and maximum performance. According to the figures, we note that there is very wide variance in the performance of detecting Sybil nodes. Especially, when the length of random route is smaller, we can observe wider variance.

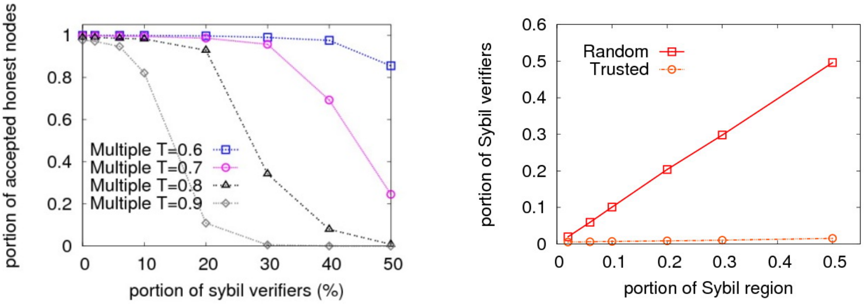
Fig. 2(b) and Fig. 2(c) represents the performance of multi-verifier based Sybil detection with various threshold, T_{thres}. In these figures, we can observe that multi-verifier based Sybil detection outperforms the single-verifier based Sybil detection in both aspects of accepting honest nodes and suppressing Sybil nodes. Also, we note that there is a tradeoff between the threshold value and the performance of multi-verifier based Sybil detection. With smaller threshold value, multi-verifier based Sybil detection accepts more honest nodes but it may accepts more Sybil nodes as well. On the other hand, with bigger threshold value, it can suppress Sybil nodes aggressively but it may not accept some honest nodes.



(a) single verifier (b) multiple verifiers - honest (c) multiple verifiers - Sybil

Fig. 2. Portion of accepted nodes as a function of the length of random route

Fig. 3(a) represents the impact of Sybil verifiers. As we can expect, when there are more Sybil verifiers, the performance of multi-verifier based Sybil detection is significantly degraded. That is, choosing honest verifiers is important to guarantee the operation of multi-verifier based Sybil detection. Fig. 3(b) shows the comparison between random verifier selection and the proposed verifier selection (Algorithm 1). In the figure, we can observe that the proposed algorithm works very well to choose honest verifiers among a social network graph where honest and Sybil nodes coexist.



(a) Portion of accepted honest nodes as a function of the portion of Sybil verifiers. Length of Random Route = 100.

(b) Portion of Sybil verifiers as a function of portion of Sybil region in a social network.

Fig. 3. Importance of trusted verifier selection. As the portion of Sybil verifiers increases, the probability of accepting honest nodes decreases.

4 Conclusion

The previous OSN based Sybil detection methods can be used for each individual node to determine whether other nodes is Sybil or not. However, it is easily observed that there is the wide variance in the performance of single verifier based Sybil detection. To eliminate this variance, this paper proposes the multi-verifier based Sybil detection, which is composed of two algorithms: 1) Selecting honest verifiers from a social network graph where honest and Sybil nodes are mixed and 2) Determining honest nodes by comparing the likelihood of acceptance of a node with a given threshold. Through the evaluation, we note that the importance of selecting honest verifiers and choosing a reasonable threshold to guarantee the performance of the proposed multi-verifier based Sybil detection method. Currently, we are working on how to choose a reasonable threshold adaptively to an arbitrary social network graph and how to improve the performance of Sybil detection.

Acknowledgement. This research was supported by the MSIP(Ministry of Science, ICT&Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (NIPA-2013-H0301-13-3005) supervised by the NIPA(National IT Industry Promotion Agency).

References

1. Danezis, G., Lesniewski-laas, C., Kaashoek, M.F., Anderson, R.: Sybil-resistant DHT routing. In: de Capitani di Vimercati, S., Syverson, P.F., Gollmann, D. (eds.) ESORICS 2005. LNCS, vol. 3679, pp. 305–318. Springer, Heidelberg (2005)
2. Sirivianos, M., Kim, K., Gan, J.W., Yang, X.: Assessing the Veracity of Identity Assertions via OSNs. In: Proc. COMSNETS 2012, Bangalore, India, January 3-7 (2012)
3. Sirivianos, M., Kim, K., Yang, X.: SocialFilter: Introducing Social Trust to Collaborative Spam Mitigation. In: Proc. IEEE INFOCOM 2011, Shanghai, China, April 10-15 (2011)
4. von Ahn, L., Blum, M., Hopper, N.J., Langford, J.: CAPTCHA: Using Hard AI Problems for Security. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 294–311. Springer, Heidelberg (2003)
5. Yu, H., Gibbons, P.B., Kaminsky, M., Xiao, F.: SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks. In: Proc. IEEE S&P 2008, Oakland, CA (May2008)
6. Viswanath, B., Post, A., Gummadi, K.P., Mislove, A.: An Analysis of Social Network-Based Sybil Defenses. In: Proc. SIGCOMM 2010 (2010)
7. Kim, K.: Sybil-Resistant Trust Value of Social Network Graph. In: Proc. the First International Conference on Smart Media and Applications (SMA 2012), Kunming, Yunnan, China, August 21-24 (2012)
8. Mohaisen, A., Hopper, N., Kim, Y.: Keep your friends close: Incorporating trust into social network-based Sybil defenses. In: Proc. IEEE INFOCOM 2011, Shanghai, China, April 10-15 (2011)