Assessing the impact of properties of a node to OSN based Sybil detection

Kyungbaek Kim
Dept. Electronics and Computer Engineering
Chonnam National University
Gwangju, South Korea
Email: kyungbaekkim@jnu.ac.kr

***Abstract*—In a distributed system, Sybil detection is important to prevent malicious users from obtaining abnormal benefits or from subvert the system. Recently, ONS-based Sybil detection methods have been proposed which does not require real world identity of users in an open distributed system. These methods use probabilistic methods such as a random walk, and the variance of the performance of Sybil detection can be easily observed. While some past researches reveal that longer random walk is required to improve the performance of OSN-based Sybil detection methods, the detail assessment of the variation of the performance still lacks. In this paper, we observe the performance of OSN-based Sybil detection in the aspects of different properties of a node, such as the coverage of a random walk and the weighted differential of the coverage. According to the observation, we assess the relationship between the node properties and the performance of OSN-based Sybil detection methods. As a result of extensive evaluation with sample social network graph, while the number of neighbors of a node is less relevant to the performance of Sybil detection, the high order of the coverage and the weighted differential of the coverage are highly correlated to the performance of OSN-based Sybil detection.**

I. Introduction

In a distributed system, defending against *Sybil attacks* is an important issue. Sybil attacks are malicious activities by generating fake identities which are called as Sybil identities belong to a malicious identity [1]. Through the Sybil attack, the malicious identity may obtain immoral gains from the distributed system or subvert the system. For example, in a peer-to-peer system, many Sybil identities join the system and they can gain the control of the system to hamper the operations of the system [2]. 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 [3], [4].

Traditional ways to defend the Sybil attack, such as CAPTCHA [5] and Verisign, uses complexity of generating identities or 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.

Recently, as an alternative approach of Sybil defense, OSN based Sybil defense methods have been proposed [6], [7]. These methods 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 (non-Sybil) region and Sybil region. According to this, these methods let a single node in a graph determine which node is Sybil or not by using a probabilistic measure such random walks. Moreover, in some researches, multiple verifiers are used to generate Sybil resistant trust value of each identity inside a social network graph [8].

However, since the OSN based Sybil detection methods rely on the probabilistic properties, the performance of detecting Sybil identities depends on some parameters used in the methods such as the length of random walk [7], [9]. While some researches showed that the hidden communities hamper the performance of Sybil detection methods, it is still a challenge to find out some properties of node which affect the performance of Sybil detection for individual nodes.

In this paper, we analyze the performance of an OSN based Sybil detection method in the aspect of various kinds of node property in a social network graph such as the number of neighbors, the coverage of a random walk, and the weighted-differential of the coverage of a random walk. Through extensive evaluations with sample real-world social network graphs, we observed that the number of neighbors is the least relevant property to the performance of Sybil detection. We also noticed that the nodes with high coverage or low weighted-differential have high probability to be considered as honest nodes by the OSN-based Sybil detection method.

II. Background

A. Assumptions of Social Network

A social network graph, $G = (V, E)$ where $|V| = N, V = v_1, v_2, ..., v_n$ and $|E| = M, e_{ij} \in E = v_i \rightarrow v_j$, is 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

This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program (NIPA-2013-H0301-13-3005) supervised by the NIPA(National IT Industry Promotion Agency)

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 [6], [9].

B. OSN based Sybil Detection Methods

We consider two types of OSN-base Sybil defense methods: SybilLimit [6], using a single verifier and RRTI (Random Route Tail Intersection) [8], using multiple verifiers. SybilLimit uses the property that in a legitimate social network graph, $G(V,E)$, the last edge, referred as the tail, traversed by a random route of $\Theta(\log|V|)$ steps is an independent sample edge approximately drawn from the stationary distribution of the graph, G. If two honest nodes draw enough number $(\Theta(\sqrt{|E|})\Theta(\log|V|))$ of tails, it follows from the generalized Birthday Paradox that sample tails intersect with high probability. The opposite holds between an honest node and a Sybil node, since of the limited number of attack edges.

For SybilLimit to detect Sybil nodes, each node prepares the sets of tails drawn by using random routes. Each node prepares the verification set of tails, S_v, which is composed of r $(= \Theta(\log|E|))$ tails drawn from random routes of length w $(= \Theta(\sqrt{|E|}))$. Also, every node generates the sample set of tails, S_s, which is compose of r tails drawn from random routes of length w. A random route is a special kind of a random walk. While a random walk randomly chooses the next node out of neighbor nodes, a random route follows the pre-defined routing table of each node. The routing table is a mapping table between incoming edges and outgoing edges. For a verifier node, v, to determine whether a suspect node, s, is an honest node or a Sybil node, the verifier node, v, compares S_v with S_s. If there is any common tails between S_v and S_s, the verifier node accepts the suspect node as an honest node. Otherwise, the verifier node considers the suspect node as a Sybil node.

We also consider the case of using multiple verifiers such as RRTI. RRTI method adapts the SybilLimit method for calculating the Sybil-resistant trust value of a node in a social graph by using multiple verifiers. The Sybil-resistant trust value of a node represents the likelihood that the corresponding node is non-Sybil, in the range from 0 to 1. RRTI method selects l verifier nodes among the pre-trusted honest nodes and each verifiers test a single suspect node whether it is an honest node or a Sybil node. The Sybil-resistant trust value is calculated by dividing the number of accepted verifiers by the number of whole verifiers. The RRTI method could be conducted by an OSN provider which has the knowledge of the entire structure of a social network graph, G, but the OSN provider does not know which nodes are honest or Sybil except few pre-trust honest nodes.

III. Properties of a node in a social network graph

The performance of SybilLimit and RRTI relies on the properties of a node in a social network graph, especially related to the properties of a random walk. It is well known that longer length of random walk is required for a node to be accepted by other nodes with higher probability, but there is still variation of performance for individual nodes which may have distinct properties to other nodes. To assess the impact of node properties for SybilLimit and RRTI, some properties of a node in a social network, G, is defined in this section. We mainly consider two kinds of node properties, such as the coverage of a random walk and the weighted differential of the coverage of a random walk, which may affect the behavior of a random walk starting from the corresponding node.

The coverage of a random walk of a node is defined as the number of nodes which can be reached by the given number of random walk process. When there is a node, v_i, a function $h_n(v_i)$ represents the set of n-hop away nodes from the node, v_i. $h_0(v_i)$ means the node, v_i, itself and $h_1(v_i)$ represents the one-hop away nodes from the node v_i, that is, the neighbor nodes of v_i. With the function $h_n(v_i)$, the coverage is defined as Equation 1.

$$C_n(v_i) = \sum_{j=0}^{n} h_j(v_i) \tag{1}$$

While the coverage represents how many nodes can be reached by a random walk, the weighted differential of the coverage of a random walk indicates the average hop count from a node to reach the majority of nodes by a random walk. Since $h_n(v_i)$ is the difference between C_n and C_{n-1}, $h_n(v_i)$ is considered as the differential of C_n. To identify the dominant differential, each $h_n(v_i)$ is normalized with the number of nodes in a social network graph, N. At last, each normalized differential is weighted by n. According to this, the weighted differential of the coverage is defined as Equation 2, where d is the diameter of a social network graph.

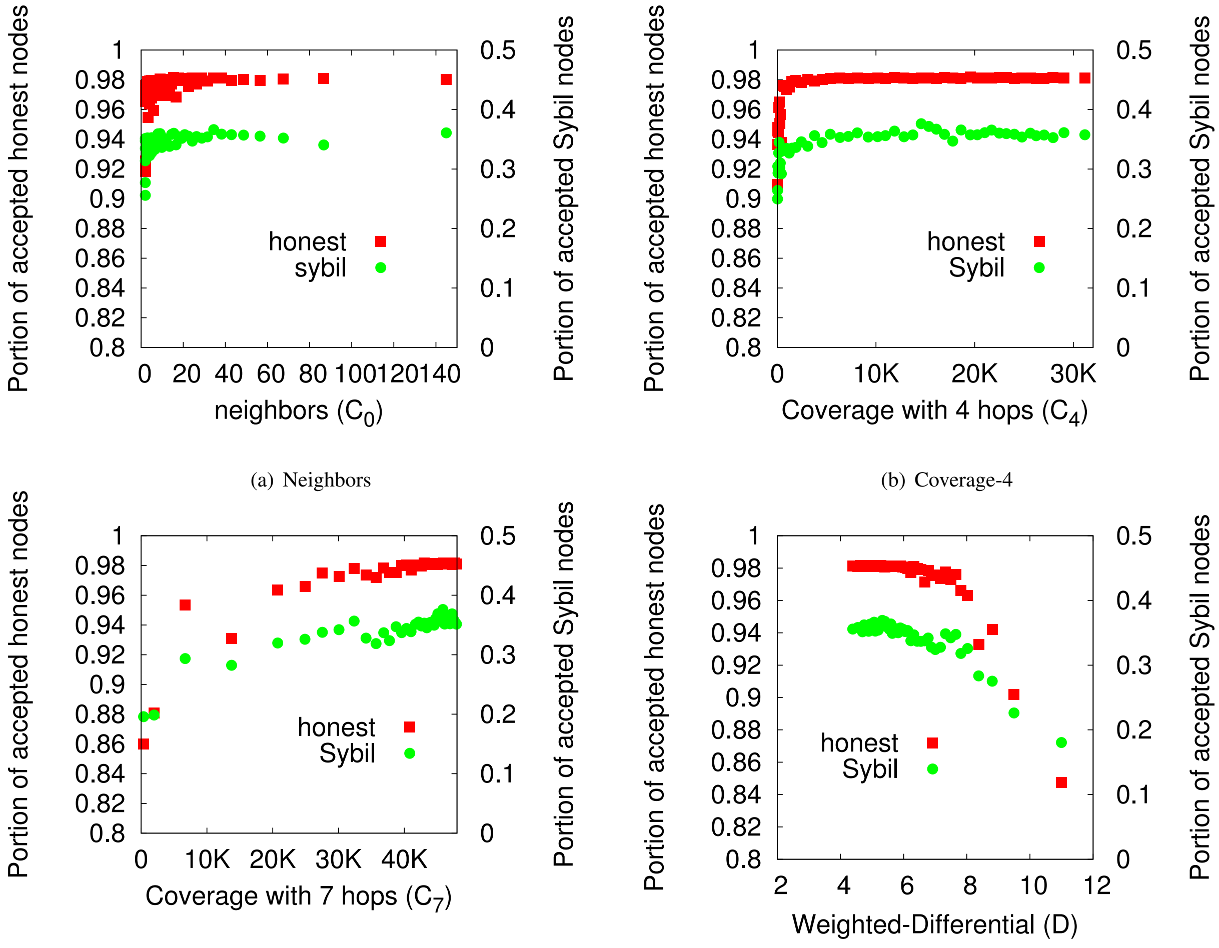
$$D(v_i) = \frac{\sum_{j=0}^{d}(j \times h_j(v_i))}{N} = \frac{\sum_{j=0}^{d}(j \times h_j(v_i))}{\sum_{j=0}^{d}(h_j(v_i))} \tag{2}$$

IV. Evaluation

To assess the impact of each node properties to OSN-based Sybil detection methods, we conducted each Sybil detection methods (SybilLimit and RRTI) on a sample social network graph which is composed of one honest region and multiple Sybil regions. As an honest region, a sample sub-graph of the Facebook social network graph is used. This sample graph has 50k nodes and 905,004 edges. The diameter of this graph is 18. Sybil regions are generated artificially. A Sybil region is generated as a single strongly connected component where the average number of neighbors is 14, and it has 2 attack edges which are connected to honest nodes randomly.

A. The case of Single Verifier

At first, we observe the performance of SybilLimit, which uses a single verifier to accept a node as an honest node. To conduct SybilLimit method, the length of a random route, w is set to 20 and the number of tails, r is set to 2000. Fig. 1 shows the portion of accepted (honest and Sybil) nodes as a function of each property of a single verifier node in a social network graph when SybilLimit is used. The considered properties of a



(a) Neighbors

(b) Coverage-4

(c) Coverage-7

(d) weighted-differential

Fig. 1. Portion of accepted nodes as a function of each property of a node in a social network graph

node are the number of neighbors ($C_0(v_i)$), the coverage with 4 hops ($C_4(v_i)$), the coverage with 7 hops ($C_7(v_i)$) and the weighted differential ($D(v_i)$).

In Fig. 1(a), we observed that the performance of the verifier nodes with low number of neighbors is arbitrary. A verifier node having 5 neighbors can achieve the similar performance of Sybil detection to the verifier nodes which has 145 neighbors. The substantial variation of the performance of SybilLimit is observed until the number of neighbors is up to around 30. That is, the number of neighbors of a node is less relevant to the performance of SybilLimit.

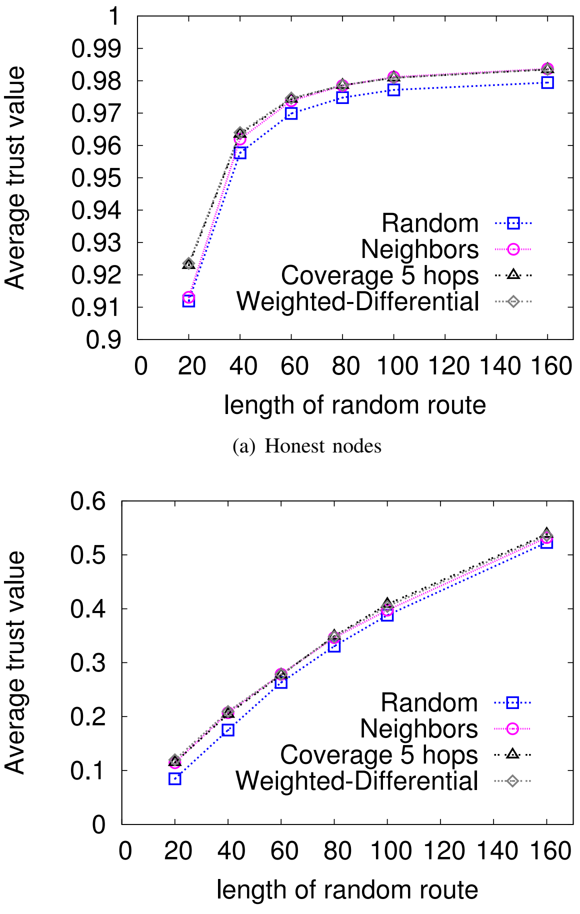
However, we can observe that the coverage with high hop counts is related to the performance of SybilLimit. When we increase the hop counts of the coverage up to 4, we can narrow down the range of variation of the performance of SybilLimit like Fig. 1(b). When the coverage with 7 hops is considered, we can see the relationship between the coverage and the performance of SybilLimit. That is, a single verifier having bigger value of coverage with 7 hops accepts more honest nodes.

In Fig. 1(d), the performance of SybilLimit is shown as a function of the weighted-differential value of a single verifier. In this figure, we observe a breakdown value of the weighted-differential. That is, a single verifier with SybilLimit works fine until its weighted-differential is below 8. If a single verifier has around 11 as the weighted-differential, it can only accept 84% honest nodes and considers other 16% nodes as Sybil nodes mistakenly. That is, to conduct SybilLimit properly, a single verifier needs to have low value of weighted-differential.

Another interesting observation is that the tendency of acceptance of Sybil nodes is similar to that of honest nodes. In Fig. 1, while the average portion of accepted Sybil nodes is much smaller than the average portion of accepted honest nodes, the shape of the function for Sybil nodes is very similar to that for honest nodes. According to this, we can note that the properties of nodes such as the coverage and the weighted differential are related to the performance of accepting not only honest nodes but also Sybil nodes.

B. *The case of Multiple Verifiers*

To assess the impact of node properties to OSN-based Sybil detection with multiple verifiers, we conduct RRTI method for calculating the Sybil-resistant trust value of a node in a social network graph. Especially, we use each node property as a basis of selecting verifiers. We considered four kinds of choosing verifiers such as random basis, the number of neighbor basis, the coverage with 5 hops basis and the



(a) Honest nodes

(b) Sybil nodes

Fig. 2. Average trust value obtained by multi-verifiers methods as a function of the length of random route. Each property of a node is used for selecting verifiers

weighted-differential basis. In the case of random basis, the verifiers are randomly chosen from honest nodes. In the case of the number of neighbor basis and the coverage with 5 hops basis, the honest nodes are sorted by each basis in decreasing order, and honest nodes having higher value are chosen. On the other hand, in the case of the weighted-differential basis, the honest nodes are sorted in increasing order, and honest nodes having smaller value are chosen. The number of verifiers, l, is set to 50 and the number of tails, r is set to 2000. The length of random route, w changes from 20 up to 160.

Fig. 2 shows the average Sybil-resistant trust vale obtained by RRTI method as a function of the length of random route. In the figures, it is easily observed that the random basis verifier selection provides lowest average of Sybil-resistant trust values, and both of the coverage basis and the weighted-differential basis verifier selection achieves highest average of Sybil-resistant trust value. The main reason of the result is that verifiers with high coverage or low weighted-differential can accept more nodes.

However, in the case of the number of neighbor basis verifier selection, when the length of random route is short such as 20, the performance is similar to that of the random basis verifier selection like Fig. 2(a). On the other hand, when the length of random route is long such as 100, the performance of the number of neighbor basis verifier selection is similar to that of the weighted-differential basis verifier selection. It is because the number of neighbor of a node is less relevant to the performance of OSN-based Sybil detection.

V. Conclusion

Defending Sybil attack is important for a distributed system to provide an open environment to users and to prevent malicious users from doing abnormal behaviors. Recently OSN-based Sybil detection methods have been proposed and users may feel free to use them to detect Sybil identities without revealing real-world identities. This paper focuses on accessing the impact of properties of nodes in a social network graph to OSN-based Sybil detection methods such as SybilLimit (a single verifier) and RRTI (multiple verifiers). The considered properties of a node are the coverage of a random walk and the weighted-differential of the coverage of a random walk. These properties of a node are mainly related to the performance of random route used by SybilLimit and RRTI. Through the extensive evaluation, we find that the number of neighbors is less relevant to the performance of OSN-based Sybil detection methods, but both of the coverage with high hop counts and the weighted-differential of the coverage are highly correlated to the performance of OSN-based Sybil detection methods. Especially, a node with high value of the coverage or the low value of the weighted-differential of the coverage can accept more nodes from the social network graph. These nodes also have high chance to accept Sybil nodes as honest nodes.

This finding of the relationship between node properties and the performance of OSN-based Sybil detection methods can be help to design a new OSN-based Sybil detection method with less variation of performance. It also may encourage the new design of algorithms of selecting verifiers for Sybil detection methods using multiple verifiers

References

[1] J. Douceur. The Sybil Attack. In *Proc. IPTPS?02*, Cambridge, MA, Mar 2002.

[2] George Danezis and Chris Lesniewski-laas and M. Frans Kaashoek and Ross Anderson. Sybil-resistant DHT routing. In *Proc. ESORICS 2005*, pp. 305–318, Milan, Italy.

[3] Michael Sirivianos, Kyungbaek Kim, Jian Wei Gan and Xiaowei Yang. Assessing the Veracity of Identity Assertions via OSNs. In *Proc. COMSNETS 2012*, January 3-7, 2012, Bangalore, India

[4] Michael Sirivianos, Kyungbaek Kim and Xiaowei Yang. SocialFilter: Introducing Social Trust to Collaborative Spam Mitigation. In *Proc. IEEE INFOCOM 2011*, April 10-15, 2011, Shanghai, China

[5] Luis von Ahn, Manuel Blum, Nicholas J. Hopper and John Langford. CAPTCHA: Using Hard AI Problems for Security In *Proc. EUROCRYPT 2003*, Warsaw, Poland.

[6] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao. SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks. In *Proc. IEEE S&P 2008*, Oakland, CA, May 2008.

[7] B. Viswanath, A. Post, K. P. Gummadi and A. Mislove. An Analysis of Social Network-Based Sybil Defenses. In *Proc. SIGCOMM 2010*, 2010

[8] K. Kim. Sybil-Resistant Trust Value of Social Network Graph. In *Proc. the First International Conference on Smart Media and Applications (SMA 2012)*, August 21-24, 2012, Kunming, Yunnan, China

[9] A. Mohaisen, N. Hopper, and Y. Kim. Keep your friends close: Incorporating trust into social network-based Sybil defenses. In *Proc. IEEE INFOCOM 2011*, April 10-15, 2011, Shanghai, China