LETTER

Two-Step Boosting for OSN Based Sybil-Resistant Trust Value of Non-Sybil Identities

Kyungbaek KIM[†a)], *Member*

SUMMARY In the design of distributed systems, defending against Sybil attack is an important issue. Recently, OSN (Online Social Network)-based Sybil defending approaches, which use the fast mixing property of a social network graph with sufficient length of random walks and provide Sybil-resistant trust values, have been proposed. However, because of the probabilistic property of the previous approaches, some honest (non-Sybil) identities obtain low trust value and they are mistakenly considered as Sybil identities. A simple solution of boosting the trust value of honest identities is using longer random walks, but this direct boosting method also increases trust values of Sybil identities significantly. In this paper, a two-step boosting method is proposed to increase the Sybil-resistant trust value of honest identities reasonably and to prevent Sybil identities from having high trust values. The proposed boosting method is composed of two steps: initializing the trust value with a reasonably long random walks and boosting the trust value by using much longer random walks than the first step. The proposed method is evaluated by using sampled social network graphs of Facebook, and it is observed that the proposed method reduces the portion of honest identities mistakenly considered as Sybil identities substantially (from 30% to 1.3%) and keeps the low trust values of Sybil identities.

key words: *Sybil attack, random walk, social network graph, Sybil-resistant trust value, boosting method*

1. Introduction

Defending against Sybil, or multiple identity, attack is an important issue in the design of distributed systems [1]. A single malicious user creates multiple identities called Sybil identities and controls them to gain abnormal profits from the participated system or to subvert the system. Traditional defenses against Sybil attacks rely on trust credentials provided by a certificate authority which requires users to present real and trusted identities such as credit cards or social security numbers. But this kind of authorization is opposite to the open membership which is one of the basic ideas of the success of distributed systems in these days.

Recent online social networks use the trust between real users embodied in social relationships to mitigate Sybil attacks. The proposed schemes mainly use properties of a social network graph to detect Sybil identities [2], [3]. The main assumption of these proposed schemes is that there is a sparse cut between the Sybil identities and honest (non-Sybil) identities in a social network graph. That is, a sufficiently long random walk starting from an honest identity in a social network graph most likely stops on another honest identity. While these schemes are generally used for a single verifier to detect Sybil identities, another kind of schemes which provides the Sybil-resistant trust value has been proposed [5]. The Sybil-resistant trust value is calculated by using multiple verifiers and used for other users to generate some parameters which need to be robust against Sybil identities. The Sybil-resistant trust value can be used for many kinds of distributed systems such as collaborative spam filtering [4], collaborative credential system [11] and p2p systems. In those systems, the Sybil-resistant trust value is used to estimate the likelihood that a participating node is trustable.

Since detecting Sybil identities by using social network structure relies on probabilistic measures such as random walks, some honest identities may obtain low Sybil-resistant trust value and be *misconceived* as Sybil identities. This mistake can be considered as the false negative in the aspect of assigning low trust value to Sybil identities. In order to minimize this false negative, the Sybil defending schemes may use the longer length of random walks as increasing the mixing time in social network graphs [6]. However, simply using the longer random walks, so called *direct boosting*, may also increases the Sybil-resistant trust value of Sybil identities significantly.

In this paper, a two-step boosting method is proposed to increase the Sybil-resistant trust value of honest identities reasonably and to prevent Sybil identities from having high trust values. The main idea of the proposed method is performing two-step calculation of Sybil-resistant trust value, that is, the separation of initializing process and boosting process. Because of this separation, the two-step boosting method can control the impact of the escaped random walk started from Sybil identities and it is possible to suppress that Sybil identities obtains very high trust value.

The purpose of the first step is assigning moderately high trust value to honest identities and low trust value to Sybil identities, and the purpose of the second step is increasing the trust value of honest identities which obtains low initial trust value. During the first step, the initial Sybil-resistant trust value is calculated by using a SybilLimit based scheme, RRTI (Random Route Tail Intersection) [5], with reasonably long random routes. During the second step, the low trust values of honest identities are boosted by being averaged over the other identities which are gathered from a social network graph where honest identities and Sybil identities are tangled. To realize the second step, two random walk based sampling methods are proposed. These methods use much longer random walks than

Manuscript received July 30, 2013.
Manuscript revised March 14, 2014.

[†]The author is with the Department of Electronics and Computer Engineering, Chonnam National University, South Korea.
a) E-mail: kyungbaekkim@jnu.ac.kr

DOI: 10.1587/transinf.E97.D.1918

the random route used in the first step, in order to visit the other identities having high trust values.

2. Two-Step Approach of Calculating Sybil-Resistant Trust Value

2.1 Assumptions

Let us consider there is a distributed system with N participating identities which form a single strongly connected social network graph, $G = (V, E)$ where $|V| = N$, $V = v_1, v_2, \ldots, v_n$ and $|E| = M$, $e_{ij} \in E = v_i \rightarrow v_j$. 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 [3], [6].

This paper focuses on the methods of calculating the Sybil-resistant trust value, t_i, which represents the likelihood that the corresponding node v_i is non-Sybil, in the range from 0 to 1 [5]. We assume that there are well-known contact points of a distributed systems called as *verifiers*. Whenever a node A wants to know the Sybil-resistant trust value of another node B, the node A gives a query to any verifier for calculating the Sybil-resistant trust value of node B. During this calculation, RRTI method [5] and the proposed boosting method are performed.

2.2 Rationale of the Two-Step Boosting

The Sybil-resistant trust value of each node v_i can be calculated by using RRTI (Random Route Tail Intersection) method [5] which adapts the SybilLimit algorithm [3]. 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 ($\Theta(\sqrt{|E|})$) 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, because of the limited number of attack edges. In RRTI method, we assume that there are l verifier nodes. Each verifier node, p_j, prepares the verification set of tails, S_{p_j}, which is composed of r $(= \Theta(\sqrt{|E|}))$ tails drawn from random routes of length w $(= \Theta(\log |V|))$. Each node $v_i (\in V)$ generates the sample set of tails, S_{v_i}, which is also composed of r tails drawn from random routes of length w. Then, RRTI calculates the Sybil-resistant trust value of a node v_i, $t_i^{initial}$, like in Algorithm 1.

With the RRTI method, honest nodes most likely obtain high initial trust value and Sybil nodes obtain low initial trust value. However, some honest nodes, especially with few neighbors or within a hidden close-knit community of the honest region [6], obtain low initial trust value, and these honest nodes are called as *misconceived honest nodes*. To compensate this misbehavior, their low Sybil-resistant trust value needs to be boosted. The simple solution of boosting their trust values is using longer random routes, so called as *direct boosting*. That is, a longer random route can pass close-knit communities and the behavior of its tail holds the stationary distribution.

Algorithm 1 Algorithm for calculating initial Sybil-resistant trust value of v_i (in V) in RRTI method

```
Require: $P = \{p_1, p_2, \ldots, p_l\}$ : set of verifiers
Require: $S_{p_1}, S_{p_2}, \ldots, S_{p_l}$ : verification sets of tails
Require: $S_{v_i}$ : sample set of tails
  $accept \leftarrow 0$
  for each $p_j$ in $P$ do
      if ( $(S_{p_j} \cap S_{v_i}) \neq \emptyset$ ) then
          $accept \leftarrow accept + 1$
  $t_i^{initial} \leftarrow \frac{accept}{l}$
```

However, using longer random routes increases the probability that a random route escapes from Sybil region as well. An escaped random route of a Sybil identity means that it may obtain a tail which locates in honest region. In direct boosting, the escaped tail can affect every verifier to accept the Sybil identity. That is, an escaped tail of a Sybil identity can increase the Sybil-resistant trust value significantly.

According to this, the separation of initialization step and boosting step is considered in order to diminish the impact of an escaped tail. During the initialization step, a reasonably long random route is used to suppress the escaping probability of random routes from Sybil identities, and assign reasonably high trust value to honest identities and very low value to Sybil identities. Then, during the boosting step, a long random walk based sampling is performed to gather the trust value of other honest nodes and the boosted trust value is calculated by averaging the gathered trust value. Unlike the direct boosting, in this two-step boosting, the trust value increases more conservatively. The escaped tail affects the boosted trust value as an additional sample value rather than a key parameter of verification, and the two-step boosting prevents Sybil identities from having very high Sybil-resistant trust value after boosting.

2.3 Boosting Sybil-Resistant Trust Value

The basic idea of boosting trust value is that gathering the trust value of other nodes and calculating the average of the gathered trust values as the boosted trust value. In this paper, two boosting methods are proposed: 1) boosting with single random route discovery, SRD (Algorithm 2) and 2) boosting with multiple random sampling, MRS (Algorithm 3).

In SRD (Single Random route Discovery) method shown in Algorithm 2, a node having lower trust value than a given threshold ($t_{threshold}$) gathers trust values of the nodes

Algorithm 2 Algorithm of boosting method with single random route discovery (SRD) for v_i (in V)

```
Require: $t_{threshold}$ : threshold of trust value
Require: $w_b$ : length of single random route
  if $t_i^{initial} \geq t_{threshold}$ then
      $t_i^{boosted} \leftarrow t_i^{initial}$
  else
      $B \leftarrow \emptyset$
      $v_c \leftarrow v_i$
      $v_p = GetRandomNeighbor(v_i)$
      for $j = 1$ to $w_b$ do
          $v_n = GetNextNodeOfRR(v_c, v_p)$
          $v_p \leftarrow v_c$
          $v_c \leftarrow v_n$
          $B.add(t_n^{initial})$
      $t_i^{boosted} \leftarrow \frac{\sum_{k=1}^{k=w_r} b_k + t_i^{initial}}{w_r+1}$, where $b_k \in B$
```

Algorithm 3 Algorithm of boosting method with multiple random sampling (MRS) for v_i (in V)

```
Require: $t_{threshold}$ : threshold of trust value
Require: $g$ : number of random sampling
Require: $w_b$ : length of a random walk
  if $t_i^{initial} \geq t_{threshold}$ then
      $t_i^{boosted} \leftarrow t_i^{initial}$
  else
      $B \leftarrow \emptyset$
      while $|B| < g$ do
          $v_j = DrawLastNodeOfRW(v_i, w_b)$
          $B.add(t_j^{initial})$
      $t_i^{boosted} \leftarrow \frac{\sum_{k=1}^{k=g} b_k + t_i^{initial}}{g+1}$, where $b_k \in B$
```

which are traversed by single random route, and calculates the average of the gathered trust values (b_k) including its initial trust value as the boosted Sybil-resistant trust value, $t_i^{boosted}$. Basically the threshold of trust value is used to decide whether a node with a trust value is a Sybil node or an honest node. In boosting methods, the threshold of trust value is used to choose nodes which may need boosting their trust value. In early research [5], it is mentioned that around 90% of honest nodes obtain higher trust value than 0.8 and all of Sybil nodes have lower trust value than 0.8 under a reasonable setting. According to this, in this paper the threshold of trust value, $t_{threshold}$, is set to 0.8 in order to boost the trust value of 10% of misconceived honest nodes. The function $GetRandomNeighbor(v_i)$ returns a random neighbor node of a node v_i, and the function $GetNextNodeOfRR(v_c, v_p)$ returns the outgoing neighbor node mapped to the incoming node v_p in the pre-defined routing table in a node v_c.

The rationale behind BSRD method is the convergence property of the random route. 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. A random route follows the given routing tables of each node, and two random routes entering an honest node along the same edge will always exit along the same edge. A random route initiated from an honest node traverses other honest nodes which have most likely high trust values. Also, it holds that all the random routes from all Sybil nodes must merge completely once they traverse the attack edge. In other words, a random route initiated from a Sybil node inside a Sybil region traverses many other Sybil nodes inside the same Sybil region, where most of Sybil nodes have low initial trust values, until it meets the attack edge.

The problem of SRD is that a random route of a Sybil node may meet an attack edge earlier and it gathers many honest nodes. To compensate this, MRS (Multi Random Sampling) method is proposed. While SRD method gathers the trust value of every traversed node by single random route, MRS method conducts multiple random walks and draws the last nodes of each random walk to gather the trust values.

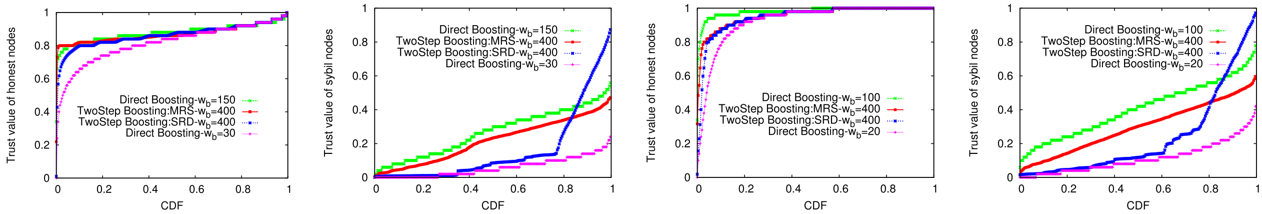
In MRS method shown in Algorithm 3, a node having lower trust value than a given threshold ($t_{threshold}$) gathers trust values of the nodes which are drawn by multiple random walk, and calculate the average of the trust values (b_k) including its initial trust value as the boosted Sybil-resistant trust value, $t_i^{boosted}$. The function $DrawLastNodeOfRW(v_i, w_b)$ returns the last visited node by a length w_b random walk starting from v_i.

3. Evaluation

To evaluate the proposed boosting methods, the Sybil-resistant trust values of nodes in a sample social network graph, which is composed of one honest region and multiple Sybil regions, are measured by using direct boosting and two-step boosting methods. As an honest region, two sample sub-graphs of the Facebook social network graph are used. Each of the sample graphs has 50K nodes (905,004 edges) and 100K nodes (1,861,360 edges), respectively. 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. That is, there are totally 50 attack edges.

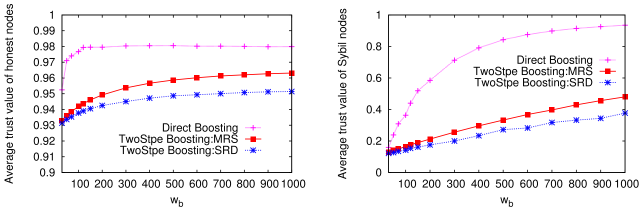
To conduct RRTI method calculating the initial Sybil-resistant trust value, it is assumed that there are previously selected verifiers in the honest region. The number of verifiers, l, is set to 50 and the number of tails, r is set to 2000. For the boosting methods, the threshold of trust value ($t_{threshold}$) is set to 0.8 and the number of random sampling of MRS method (g) is set to 49.

To observe the performance of the proposed boosting methods, Fig. 1 shows the distribution of Sybil-resistant trust value of honest and Sybil nodes with different boosting methods. That is, the x axis of figures represents the cumulative density function for a trust value. In Fig. 1, it is observed that the direct boosting with longer random routes (DirectBoosting-w_b = 150) increases the trust value of hon-



(a) Honest nodes - 100K graph
(b) Sybil nodes - 100K graph
(c) Honest nodes - 50K graph
(d) Sybil nodes - 50K graph

Fig. 1 Distribution of Sybil-resistant trust values of honest and Sybil nodes with different boosting methods.



(a) Honest nodes
(b) Sybil nodes

Fig. 2 Sybil-resistant trust value of 50K graph as a function of the length of random walks/routes, w_b.

est nodes than DirectBoosting-w_b = 30, but it also increase the trust value of Sybil nodes significantly like Fig. 1 (b). However, the proposed boosting methods increase the trust value of honest nodes significantly, and they keep the trust value of Sybil nodes low. In Fig. 1 (a), while the portion of misconceived honest nodes having low trust value (< 0.8) of DirectBoosting-w_b = 30 is 30%, the portion of misconceived honest nodes of TwoStep Boosting:MRS-w_b = 400 is only 1.3%. Moreover, this improvement of TwoStep Boosting:MRS-w_b = 400 on 100K graph outperforms the performance DirectBoosting-w_b = 150, in both aspects of obtaining high trust values of honest nodes and adhering low trust values of Sybil nodes.

Figure 2 shows the average trust value of honest and Sybil nodes with various length of random walks/routes, w_b. The performance of boosting methods (Direct boosting and TwoStep boosting-MRS/SRD) rely highly on the length of random walks/routes. However, the saturation position of two-step boosting methods is different to the direct boosting. Since the impact of the escaped tail is significant in the direct boosting method, the trust value boosted by the direct boosting method is saturated earlier than the two-step boosting methods. In other words, in the two-step boosting methods, the impact of escaped tail is not significant. Consequently, more sophisticated control of boosting trust values become possible.

4. Related Works

Recently, OSN-based Sybil defending methods are proposed [2], [3], [5], [7]–[10]. Some of them use the fast mixing properties of random walks on a social network graphs to detect Sybil identities, but the performance of these methods rely on the length of the random walks [2], [3], [5]. Few researches have focused on the effect of the length of the random walks and reveals that the close-knit communities in the honest region are the main reason of requiring longer walk to guarantee the correct Sybil defense [6], [8]. However, using longer random walk may hamper the performance of Sybil-defense. This paper mainly focuses on how to minimize the portion of misconceived honest identities without losing Sybil-defense properties.

5. Conclusion

This paper proposes a new approach to boosting the Sybil-resistant trust value of honest (non-Sybil) identities and keeping the low trust value of Sybil identities. The proposed approach has two steps of calculating the Sybil-resistant trust value: 1) RRTI — initializing the trust value and 2) boosting trust value with SRD or MRS. While random walks/routes can be used for both steps, it is preferred that using shorter length of random walks/routes for initializing the trust value and using much longer length of random walks/routes for boosting the trust value. Through the evaluation with the sample social network graphs of Facebook, it is observed that the proposed boosting method can boost the trust value of honest identities substantially and keep the low trust value of Sybil identities.

Acknowledgements

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2014-H0301-14-1014) supervised by the NIPA (National IT Industry Promotion Agency).

References

[1] J. Douceur, “The Sybil attack,” Proc. IPTPS02, Cambridge, MA, pp.251–260, March 2002.
[2] H. Yu, M. Kaminsky, P.B. Gibbons, and A. Flaxman, “SybilGuard: Defending against Sybil attacks via social networks,” Proc. SIGCOMM06, Pisa, Italy, pp.267–278, Sept. 2006.
[3] H. Yu, P.B. Gibbons, M. Kaminsky, and F. Xiao, “SybilLimit: A near-optimal social network defense against Sybil attacks,” Proc. IEEE S&P 2008, Oakland, CA, pp.3–17, May 2008.
[4] M. Sirivianos, K. Kim, and X. Yang, “SocialFilter: Introducing social trust to collaborative spam mitigation,” Proc. IEEE INFOCOM 2011, Shanghai, China, pp.2300–2308, April 2011.
[5] K. Kim, “Sybil-resistant trust value of social network graph,” Proc.

First International Conference on Smart Media and Applications (SMA 2012), Kunming, Yunnan, China, pp.1–4, Aug. 2012.

[6] A. Mohaisen, N. Hopper, and Y. Kim, "Keep your friends close: Incorporating trust into social network-based Sybil defenses," Proc. IEEE INFOCOM 2011, Shanghai, China, pp.1943–1951, April 2011.

[7] N. Tran, B. Min, J. Li, and L. Subramanian, "Sybil-resilient online content voting," Proc. NSDI 2009, pp.15–28, 2009.

[8] B. Viswanath, A. Post, K.P. Gummadi, and A. Mislove, "An analysis of social network-based Sybil defenses," Proc. SIGCOMM 2010, pp.363–374, 2010.

[9] N. Tran, J. Li, L. Subramanian, and S.S.M. Chow, "Optimal Sybil-resilient node admission control," Proc. INFOCOM 2011, pp.3218–3226, 2011.

[10] C. Lesniewski-Laas and M.F. Kaashoek, "Whanau: A Sybil-proof distributed hash table," Proc. NSDI 2010, pp.111–126, 2010.

[11] M. Sirivianos, K. Kim, J.W. Gan, and X. Yang, "Assessing the veracity of identity assertions via OSNs," Proc. COMSNETS 2012, pp.1–10, 2012.