Sybil-aware Least Cost Rumor Blocking in Social Networks

Yabin Ping*, Zhenfu Cao*, Haojin Zhu*
*Shanghai Jiao Tong University, Shanghai 200240, P. R. China
*{ybping, zfcao, zhu-hj}@sjtu.edu.cn

Abstract—**Rumor blocking and Sybil Attack are regarded as two main security threats in online social networks. The existing work on rumor blocking mainly considers how to minimize the number of protectors used to protect bridge ends. In this study, our experiments based on the Twitter data set show that the existence of the sybil users will dramatically reduce the effectiveness of the rumor blocking by 30%. Motivated by this, we propose a novel sybil-aware least cost rumor blocking framework which jointly considering how to minimize the impact sybil attacks on rumor blocking and optimize the rumor blocking effectiveness. The proposed SLCRB algorithm is well demonstrated by extensive simulations and discussions.**

Keywords – **least cost rumor blocking; sybil attack; social networks**

I. Introduction

The large scale social networks (e.g., Facebook, Twitter, SinaWeibo, Wechat) are emerging as a kind of new platform, which allows the information propagation and ideas exchange to influence a large population in a short period of time [2]. OSNs (Online Social Networks) like Facebook and Twitter are reshaping the way people take collective actions, which can be witnessed by the fact that OSNs have played a crucial role in the recent uprisings of the “Arab Spring” and the “London Riots”. It is also pointed out the existing researches that social networks ease the spread of rumors [4]. A latest example is about the missing Malaysia Airlines flight MH370. Due to the absence of timely authoritative information, and fast propagation of social networks (e.g., Sina Weibo and Wechat), numerous rumors have been spawned, most of which cannot be verified and make massive efforts squandered.

Sybil attacks [7][8] are regarded as another main threat for social network security. Sybil attackers (or social bots, spammers) are defined as software-controlled OSNs accounts that mimic human users with malicious intentions. For example, according to a article in Bloomberg Businessweek in May 2012, as many as 40% of the accounts on Facebook, Twitter, and other popular OSNs are spammer accounts (or social bots), and about 8% of the messages sent via social pages are spams, approximately twice the volume of six months ago. It is also pointed out that sybil users play an important role in the spam campaign, which may potentially lead to phishing, malware, and scams or even political astroturf [5][6], which refer to campaigns disguised as spontaneous, popular “grassroots” behavior that are actually carried out by a single person or organization.

Rumor propagation and sybil attacks are inherently correlated, which foster the fast spreading of rumors. Previous researches have investigated the rumor blocking problem by assuming the rumors and the protectors are following the same diffusion mechanism, and trying to block a certain number of links in a network to reduce the terrible results caused by rumors. In [4], it investigates the problem of minimizing the number of protectors used to protect bridge ends, which is called Least Cost Rumor Blocking (LCRB) problem.

However, the existing rumor blocking methods failed to consider the impact of sybil attacks on the rumor blocking, which renders their proposed solutions less effective in the presence of sybil attacks. The existing rumor blocking solutions relied on the selection of protectors to prevent the rumors from further propagation, but they cannot enforce sybil users to honestly perform the rumor blocking job. Therefore, existence of sybil users will seriously disrupt the effectiveness of the existing rumor blocking solutions. In section VI, our experiments will demonstrate that, for the Twitter dataset, the sybil attacks will reduce the effectiveness of rumor blocking algorithm by about 30%.

To achieve sybil-aware rumor blocking, one straightforward approach is identifying the sybil accounts firstly and then performing the rumor blocking. However, this approach will face the difficulty of determining whether a specific node is sybil node with a high confidence. Different from previous researches, we propose a novel sybil detection and rumor blocking framework, which jointly consider the network structure and the probability of being a sybil node in this social network and then choose the most appropriate nodes to block rumor propagation.

The contributions of this paper are summarized as follows:

- We identify a new sybil attack, towards existing rumor blocking algorithms.
- We propose a novel sybil attack-aware rumor blocking framework. The basic idea of the proposed framework is assigning a weight to each node based on its possibility of being a honest node, and proposing a new protector selection algorithm based on node's importance of spreading the information as well as its possibility of being a honest node. Our new framework could achieve both rumor blocking and reducing the negative effectiveness of sybil attacks.
- We implement it on the Twitter dataset and the evaluation results validate the effectiveness of the proposed attack.

978-1-4799-3512-3/14/$31.00 ©2014 IEEE

- We compare the proposed algorithm with the existing work. The evaluation results demonstrate the efficiency and effectiveness of the proposed work.

The rest of this paper is organized as follows: In Section II presents related works, followed by system models and a detail description of algorithms in Section III. Next, in Section IV we explain our ground-truth data set of real-social network and our experiment greets us with a sobering results. Section V offers our conclusions and points the directions of possible future research.

II. Related Work

To the best of our knowledge, the influence diffusion problem was first studied by [10][11], in which Richardson and Domingos explored the IM problem as an algorithmic problem. And in [12][13] the authors further translated IM problem into an optimization problem. Their work is a milestone for subsequent research on IM problems [14]. However, those researchers didn't consider the aspects of real-social networks. In [4], the authors studied two variants of the LCRB problem in social networks under the DOAM model (LCRB-D problem) and the OPOAO (LCRB-P problem) respectively. However the authors of [4] ignored the sybil nodes in the social networks, which have drawn increasing researcher's attention in both academia and industry [3] [7][8][17].

III. System Model

In this section, we give the definition of Sybil-aware Least Cost Rumor Blocking Problem (SLCRB) as well as our system model. Without loss of generality, we model the considered social network topology as a directed graph $G = (V, E)$ consisting of $|V|$ vertices and $|E|$ edges, vertices V representing individuals of the social network and edges E representing trust relationships among the individuals. For any two nodes $v_i, v_j \in V$, a directed edge $(v_i, v_j) \in E$ means individual v_i has the impact on individual v_j. If v_i is controlled by a malicious user, v_i is regarded as a sybil node, and such an edge connecting an honest community and a sybil community is referred to as an *attack edge*. Honest community contains all honest nodes and sybil community contains all sybil identities created by malicious users as shown in Fig.1.

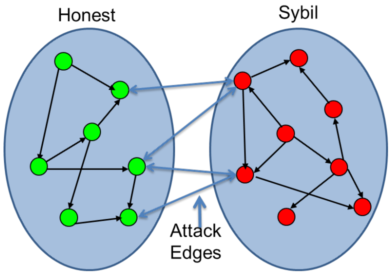
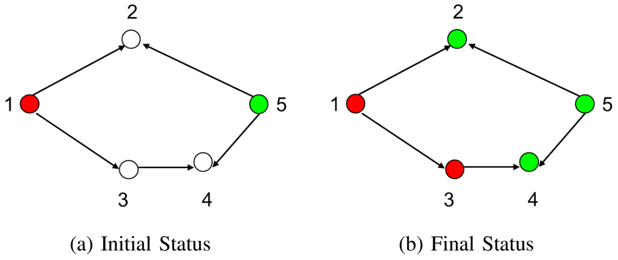


Fig. 1. The community with honest nodes and sybil nodes. Note that the social network is consisting of many communities, and an edge across an honest community and a sybil community is an attack edge.

As shown in [9], a social graph is composed of a set of small communities, denoted as$C_1, C_2, ..., C_k$. These communities satisfy $\cup_{i=1}^{k} C_i = V$ and each pair of C_i, C_j is disjoint. Each small community is densely connected inside while sparsely connected among various communities. This is because people in the same community share the common features or interests such as food, reading, or travel. So the influence spreads faster within a community, but much slower among different communities. We follow the same definition as [4] that the community containing rumor originators is a rumor community and the neighbor communities of rumor community are R-neighbor communities. The rumors originated from one community spread fast within its own community. Therefore one promising approach to prevent rumors from diffusing to R-neighbor communities is choosing bridge ends or protectors that are the boundary nodes of R-neighbor communities [4]. It is important to point out that these bridge ends or protectors could be sybil nodes, which may refuse to stop these rumors for their own benefits (e.g., increasing their influence which is important to water army).



(a) Initial Status (b) Final Status

Fig. 2. At the initial status Fig.(2a) there is only one rumored node (node 1) and one protected node (node 5) respectively. At the final status Fig.(2b), follow the above rules (2)(5) nodes 3,4 are affected by nodes 1 and 5 respectively. And based on rule 4, so the node 2's final status is protected.

Before presenting our system model, we give some definition similar to [4].

Definition 1: Bridge ends: Bridge ends is such a set, in which each node has at least one direct in-neighbor in C_r (rumor originators community, which is predetermined) and is reachable from rumors.

Definition 2: Sybil-aware Least Cost Rumor Blocking problem (SLCRB): Given a community C_r, a set of rumor originators $S_R \in C_i$ and bridge ends B, SLCRB problem is to find least number of nodes as protector originators which can protect all of the bridge ends when there are sybil attacks in social networks.

This diffusion model follows the following rules (Demonstrate in Fig.2):

(1) A node in the social graph has four status: protected (will not propagate rumor), rumored (will propagate rumor), inactive (not protected or rumored), sybil(will propagate rumor).

(2) A protected node will protect its neighbor nodes from rumored.

(3) A rumored node will propagate the rumor to its neighbor nodes with probability 1.

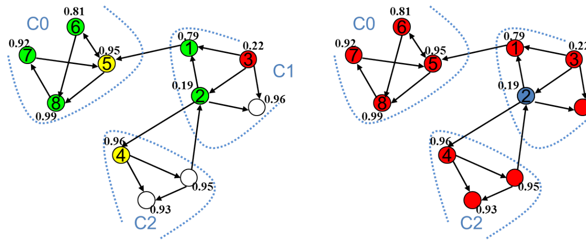
(4) A protected node has higher priority than a rumored node when they impact a node at the same time.

(5) A sybil node will propagate the rumor to its neighbor nodes with high probability (Demonstrate in Fig.(3b)).

IV. Demonstration of The Impact of Sybil Attack on Rumor Blocking

Sybil attacks are defined as the malicious users who try to create multiple identities in order to increase their own influence in a distributed system. Sybil attacks are found widely, and there has been interest in leveraging social network structure to defend sybil attacks recently. Though the malicious users can create many identities, due to the human efforts involved for establishing the attack edge, it is difficult to build the connections between a rumor community and an honest community in social networks. This makes the cut of attack edges small as pointed out in [7][8][17].

If there is a directed edge from v_i to v_j, it means that individual v_i will have impact on individual v_j. v_j is assumed to believe whatever v_i tells him in normal case, because they are trusted. However, if v_i is a sybil node which is controlled by a malicious user, v_i can forward a rumor to v_j, which can propagate this message to his other friends, and so on until the whole network is propagated or the rumor meets a protector (rumor blocking). According to our system model, if there are sybil nodes that are chosen as the protectors of bridge ends, the LCRB algorithm will fail.



(a) Normal Case

(b) Sybil Attack Case

Fig. 3. The float number beside each node is the probability of this node being honest, denoted as P_v. If $P_v \leq \delta$ (a system threshold) we say node v is a sybil node with high probability. In Fig.(3a) Red node 3 is rumor node; Yellow nodes 4,5 are Bridge ends; Green nodes 1,2,6,7,8 are protector nodes; If set $\delta = 0.3$, so in Fig.3, the node 2 is a sybil node.

Now we will explain the process by using the following example. In normal case of LCRB, the basic idea is to prevent the rumor originators from spreading the rumors out of its own community. So in Fig.(3a) we can choose protector set $\{2\}$ to protect the bridge ends 4 and 5. By this way, the rumor can not be spread to the community C_0 and C_2. However, if the protector node 2 is actually a sybil node, as shown in Fig.(3b), the whole communities C_0 and C_2 will be affected, because node 2 will diffuse the rumor. However if we can judge node 2 is a sybil node with a high confidence we can exclude node 2 as a protector, instead we choose protector set $\{1, 4\}$. As a result, the whole communities C_0 and C_2 will not be affected.

In our experiments, the results show that about 25% of bridge ends are sybil nodes and 27% of protectors are sybil nodes on average when performing LCRB algorithm and about 31.3% to 44.9% nodes are affected within only 3 hops in the presence of sybil nodes. On the other hand, there are only 12.2% to 17.4% nodes are affected when perfroming SLCRB algorithm, which can demonstrate the efficiency of our new framework.

V. Algorithm

A. The Overview of SLCRB Algorithm

In this section, we give an overview of the proposed **Algorithm 1** SLCRB algorithm. The algorithm includes two stages: Sybil Detection Stage, in which we determine the probability of a specific node being sybil or honest, and Protector Selection Stage, in which we select the bridge ends and protectors by considering both their importance of rumor blocking and their probability of being a sybil node.

We consider the communities of social graph $C = \cup_{i=1}^{k} C_i$ and initial rumor originators SR. We use the BFS (Breadth-First Search) method to find out the bridge ends, denoted as SB. Then based on SB as well its probability of being the sybil nodes, we could adopt the BBFS (Backward Breadth-First Search) algorithm to find out the protector blocking set on the bridge ends, denoted as PB. At last, we propose a greedy set cover algorithm to select all possible least protector cover set SC, then calculte the average probability of each cover set $\overline{P}_{SC_i} = \sum_{v \in SC_i} P_v / |SC_i|$. We choose the SC_i which has highest average probability to block the rumor.

In the follows, we utilize the below example to illustrate how the proposed SLCRB works, as shown in Fig.3. The float number beside each node is the probability of this node being honest, denoted as P_v. If $P_v \leq \delta$ (a system threshold) we say node v is a sybil node. In this example we set $\delta = 0.3$, so in Fig.3, the node 2 and 3 are sybil nodes, and the rest nodes are honest nodes. Now given $C = \{C_0, C_1, C_2\}, SR = \{3\}$, so $SB = \{4, 5\}, PB_1 = \{5\}, PB_2 = \{4, 5\}, PB_4 = \{4\}$, $PB_5 = \{5\}, PB_6 = \{5\}, PB_7 = \{5\}, PB_8 = \{5\}$. Then we remove the sybil protector candidate PB_2. Finally, according to the greedy set cover algorithm we know the protector set can be $SC_1 = \{1, 4\}, SC_2 = \{4, 5\}, SC_3 = \{4, 6\}, SC_4 = \{4, 7\}$, or $SC_5 = \{4, 8\}$. After calculating the average probability of each set we choose the $SC_5 = \{4, 8\}$, because it has the maximum average probability 0.975.

B. Sybil Detection Stage

In this section, we discuss **Algorithm 2** used to label each node's status (e.g., honest or sybil), based on the Bayesian inference to detect the approximate attack edge cuts, which has been proposed in [8]. Labeling each node's status mainly includes three steps. The first step is generating a set of random walks on a social graph. The second step is using MH (Metropolis-Hasting algorithm) [8][18] to sample honest configurations. Finally, according to the N samples $X_i (1 \leq i \leq N)$ generated by the second step, we can calculate the marginal probability of each node's status.

As pointed out by [7], a random walk on the social graph converges quickly to a node following the stationary distribution of the graph (e.g., $log|V|$ steps). In order to generate enough random walk traces, we will perform S random walks

Algorithm 1 SLCRB Algorithm

```
INPUT: A directed graph $G = (V, E)$, a community set $C = \{C_1, C_2, ...C_k\}$, a rumor initial set $SR = \{r_1, r_2, ..., r_m\} \subseteq V(C_i)$
    // $V(C_i)$ represent the vertices in $C_i$
OUTPUT: A Protector set $SC \subseteq V$;
for each v in $SR$ do
    Find all bridge ends with high probability to be honest node in G by BFS (Breadth-First-Search) method, denoted as a set $SB$
end for
for each v in $SB$ do
    Find all in-neighbors $w \in N^i(v)$ of $v$, where i is determined by the value of the shortest paths between v and any node $w \in SR$, denoted as a set $Q_v$
end for
From $Q_1, Q_2, ..., Q_v$ find bridge ends that each candidate can protect, denoted as a set $PB_1, PB_2, ..., PB_u$.
Apply greedy algorithm on $PB_1, PB_2, ..., PB_u$ to find all possible least protector cover set on bridge ends $SB$, denoted as a set $SC_i, 1 \leq i \leq k$
for each $SC_i$ do
    Calculate $\overline{P}_{SC_i} = \sum_{v \in SC_i} P_v / |SC_i|$
end for
Return OUTPUT Max($SC_i$)
```

on each vertex first [8], then we will get $S \cdot log|V|$ random walks totally. We denote each random walk as a vertex_pair $< start\_vertex, end\_vertex >$ and denote all vertex_pairs as a set T. Therefore we define our probability transition matrix as follows:

$$P_{ij} = \begin{cases} \dfrac{1}{d_{iout}} & \text{if } (v_i, v_j) \in E \\ \\ 0 & \text{otherwise} \end{cases}$$

where d_{iout} is the out-degree of vertex i in G.

A random walk from an honest community X is less likely to end up in a dishonest community $\overline{X}$, because there is a small cut between them. Fig.4 illustrates the transition probabilities between honest X and dishonest $\overline{X}$ regions of the social network. According to the Bayes theorem:

$$P(X = Honest|T) = \frac{P(T|X = Honest) \cdot P(X = Honest)}{Z}$$

where $Z = \sum_{X \subset V} P(T|X = Honest) \cdot P(X = Honest)$.

Based on [8], instead of directly calculating $P(T|X = Honest)$, we use an approximate probability calculated by random walk traces data, that is:

$$\begin{aligned} P(T|X = Honest) = {} & (P_{XX})^{N_{XX}} \cdot (P_{X\overline{X}})^{N_{X\overline{X}}} \\ & \cdot (P_{\overline{XX}})^{N_{\overline{XX}}} \cdot (P_{\overline{X}X})^{N_{\overline{X}X}} \end{aligned}$$

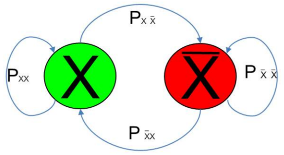


Fig. 4. Illustrate transition probabilities between honest X and dishonest $\overline{X}$ regions of the social network.

Here, $P_{X\overline{X}}$ and $P_{\overline{XX}}$ are defined as follows:

$$P_{X\overline{X}} = \frac{N_{XX}}{N_{XX} + N_{X\overline{X}}} \cdot \frac{1}{|X|}$$

$$P_{\overline{XX}} = \frac{N_{\overline{XX}}}{N_{\overline{XX}} + N_{\overline{X}X}} \cdot \frac{1}{|\overline{X}|}$$

Computing

$$\sum_{X \subset V} P(T|X = Honest) \cdot P(X = Honest)$$

requires much cost, because it involves an exponential number of items in the size of V. So we adopt MH (Metropolis-Hasting algorithm) [8] to sample other X which follows the above distribution. And the new sample $X^{'}$ is accepted to replace X with probability α:

$$\alpha = min(\frac{P(X^{'}|T) \cdot Q(X|X^{'})}{P(X|T) \cdot Q(X^{'}|X)}, 1)$$

We use the same method with [8] to calculate Q.

Now we propose **Algorithm 2**

Algorithm 2 Sybil Detection Algorithm

```
INPUT: A directed graph $G = (V, E)$, an honest initial set $S_P = \{p_1, p_2, ..., p_m\} \subseteq V(C_i)$ //$S_P$ must contain at least one nodes.
OUTPUT: the probability of each node being honest.
for each $v$ in V do
    $start\_vertex = v$
    for loop = 1 to $log|V|$ do
        Record $end\_vertex$ of random walk start from $start\_vertex$
        Add $< start\_vertex, end\_vertex >$ to set T
    end for
    Use MH (Metropolis-Hasting algorithm) to sample N honest configurations $X_i \sim P(X|T)$
    for each $v$ in V do
        $P_v = \frac{\sum_{j \in [0, N-1)} I(v \in X_j)}{N}$
        //$\delta$ is a threshold pre-defined by the system
        if $P_v > \delta$ then
            We say $v$ is an honest node with a high probability
        else
            We say $v$ is a sybil node with a high probability
        end if
    end for
end for
Return OUTPUT $\{P_v\}, v \in V$
```

Here, $I(v \in X_j)$ is an indicator function, which is defined as follows:

$$I(v \in X_j) = \begin{cases} 1 & \text{if } v \in X_j \\ \\ 0 & \text{otherwise} \end{cases}$$

C. Complexity Analysis of The Proposed Algorithm

It has been proved that the LCRB-D problem is equivalent to the SC (Set Cover) problem [4]. As we all know, optimization version of set cover problem is NP-hard, so we must use an approximate algorithm for this problem. Fortunately, there is a polynomial time $O(log|V|)$ factor approximation, where $|V|$ is the number of nodes in Bridge ends. As a result, the complexity of Algorithm 1 is $O(log|V|)$. Now we are going to analyse the complexity of Algorithm 2. There are total $|V|$ nodes in the social graph, and each node performs S times random walk, the length of which is $log|V|$. So the complexity of Algorithm 2 is $S \cdot |V| \cdot log|V|$. In our experiment, S is set to $log|V|$, so the complexity is $|V| \cdot (log|V|)^2$.

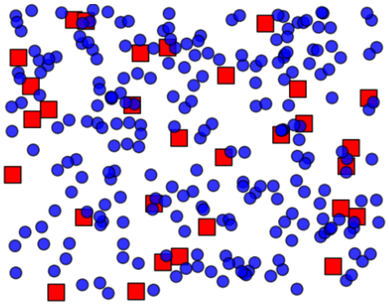


Fig. 5. The normal users and sybil users are denoted as blue-dots and red-squares, which scattered in the whole space.

VI. Evaluations

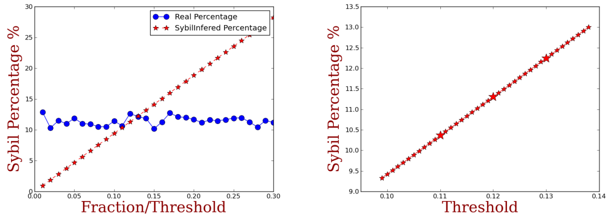
A. Date-set

In our experiments, we use the real-world data from Twitter, a well-known OSN website, to evaluate the effectiveness of the proposed algorithms. The public available data-set [2] consists of 41.7 million nodes (individuals) and 1.47 billion edges (social relationships). Due to the huge size of total data, we use only a sub-network for our evaluation. The sub-network is picked as follows. First, we randomly select 3 seeds from all of the nodes and add them to a queue. Then we pop a node from the queue and traverse the whole social network to search its neighbor nodes. If such a neighbor is found, we push it into the queue. Third we use the Breadth-First-Search method to get all neighbors within three hops. The picked sub-network contains 403355 edges, and we remove duplicate edges and the nodes with degree (in-degree or out-degree) less than 5. At last we totally get 369590 edges with 33516 nodes.

B. The Evaluation on Sybil Detection Algorithm

As the first step of evaluation, we use experiments to evaluate the effectiveness and efficiency of the sybil detection algorithm. Fig.5 shows the evaluation results. The blue-dot nodes represent the normal user nodes, and the red-square nodes are sybil user nodes. In Fig.5, we show a fragment of the adopted data set. In this figure, the normal users and sybil users are indicated in blue-dot and red-square, which scattered in the whole space.

We further evaluate the impact of network size on the effectiveness of the sybil detection. To achieve this, we tune the network size, which starts from 5%, then to 10%, 15%, 20%, 25%, 30%. We validate the sybil distribution by using the Twitter API to query these nodes' status, sybil or normal. Based on the results, it shows that the percentage of the sybil nodes varies in the range $(10\%, 13\%)$. We call Twitter's check results as real percentage of sybil nodes, and the results are depicted with blue-dot solid line in Fig.(6a).



(a) Sybil Percentage

(b) Threshold δ

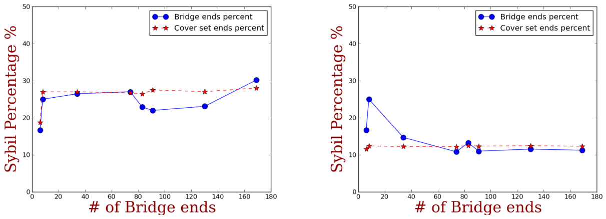
Fig. 6. In Fig.(6a) compare the real percentage of sybil nodes get from Twitter API with our own sybil detection results. As a reference we zoom the sybil detection results as Fig.(6b)

Then, we would like to investigate how to choose the threshold δ to achieve a desirable sybil detection rate. The rationale behind this experiment is shown as follows. If setting the threshold δ too small (e.g., less than 0.1), it will obtain a very high false negative, because the random walk will travel most of nodes multiple times. On the other side, if setting the threshold δ too large, a high false positive will make the sybil detection results less desirable, because some normal nodes will be wrongly treated as the sybil ones. We plot the relationship between the chosen threshold and sybil detection percentage in Fig.6. It is observed that if choosing the threshold δ within $(10\%, 14\%)$, the detection percentage is in line with the real percentage obtained from Twitter API. Therefore, in the subsequent sections, we will set δ to 0.13 as the corresponding parameter setting.

C. Evaluation Results

In this section, we show our scheme SLCRB's efficiency and effectiveness. Fig.(7a) illustrates the LCRB results without considering sybil attacks. The Y-axis represents the percentage of sybil nodes, while the X-axis represents the number of bridge ends or the number of protectors, which are output by Algorithm 1. The blue-dot solid line and red-star dashed line represent the percentage of sybil nodes on the bridge ends and protectors respectively. After checking these nodes' status, we find that about 25% of bridge ends are sybil nodes and 27% of protectors are sybil nodes on average.

In Fig.(7b) we show our SLCRB's results which consider the sybil attack in rumor blocking. From the experiment results, it is observed that a significant percentage of sybil nodes are identified for both on bridge ends and protectors, which are 10% and 11%, respectively. These sybil nodes will seriously disrupt the effectiveness of the existing rumor blocking algorithm such as [4].



(a) LCRB

(b) SLCRB

Fig. 7. This figure demonstrate the percentage of the sybil nodes on the bridge ends (blue-dot solid line) and on protector cover set (red-star dashed line).

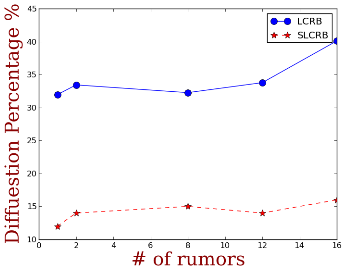


Fig. 8. Illustrate the diffusion rate

Lastly, we compare the proposed SLCRB algorithm with the previous rumor blocking algorithms in terms of the rumor prevention in the presence of sybil attacks. With different initial numbers of rumor nodes, we let both rumor and protector nodes propagate their effect within 3 hops based on our system model. Because we get our sub-network within 3 hops by each node and its neighbors, so any node of the whole sub-network can be reached within 3 hops. Then we count the number of nodes which are infected by rumors. As shown in Fig.8, if choosing LCRB algorithm, we can observe that about 31.3% to 44.9% nodes of the sub-network are affected within 3 hops in the presence of sybil nodes (blue-dot solid line). On the contrary, if choosing the proposed SLCRB algorithm, only 12.2% to 17.4% nodes are affected (red-star dashed line), which further demonstrates the advantage of the proposed SLCRB algorithm.

VII. Conclusion

In this paper, we present sybil-aware least rumor blocking problem and propose an efficient and effective algorithm SLCRB. In SLCRB we integrate the rumor blocking with sybil attack in social networks, thus when performing the rumor blocking we consider the probability of key nodes (e.g., bridge end or protector) being honest or sybil. Not only do we make an analysis of SLCRB, but also do some experiments to evaluate it. Our experiments on a real-world social network show that sybil nodes seriously disrupt the effectiveness of the existing rumor blokcing, and we demonstrate the advantage of the proposed SLCRB algorithm by comparing it with existing algorithms.

Acknowledgement

We greatly appreciate the insightful comments and constructive feedback from the anonymous reviewers. And this work is supported by the National Natural Science Foundation of China (Grant No. 61371083, 61373154, 61033014, 61272444 and 61161140320), the Prioritized Development Projects of the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20130073130004).

References

[1] Zhang J, Zhang R, Zhang Y, et al. On the impact of social botnets for spam distribution and digital-influence manipulation[C]//Communications and Network Security (CNS), 2013 IEEE Conference on. IEEE, 2013: 46-54.

[2] Kwak H, Lee C, Park H, et al. What is Twitter, a social network or a news media?[C]//Proceedings of the 19th international conference on World wide web. ACM, 2010: 591-600.

[3] Alvisi L, Clement A, Epasto A, et al. Sok: The evolution of sybil defense via social networks[C]//Security and Privacy (SP), 2013 IEEE Symposium on. IEEE, 2013: 382-396.

[4] Fan L, Lu Z, Wu W, et al. Least cost rumor blocking in social networks[C]//Distributed Computing Systems (ICDCS), 2013 IEEE 33rd International Conference on. IEEE, 2013: 540-549.

[5] J. Ratkiewicz, M. Conover, M. Meiss, B. Gonc alves, A. Flammini, and F. Menczer, Detecting and tracking political abuse in social media, in ICWSM11, 2011.

[6] J. Ratkiewicz, M. Conover, M. Meiss, B. Gonc alves, S. Patil, A. Flam- mini, and F. Menczer, Truthy: mapping the spread of astroturf in microblog streams, in WWW 11, 2011, pp. 249252.

[7] Yu H, Kaminsky M, Gibbons P B, et al. Sybilguard: defending against sybil attacks via social networks[J]. ACM SIGCOMM Computer Communication Review, 2006, 36(4): 267-278.

[8] Danezis G, Mittal P. SybilInfer: Detecting Sybil Nodes using Social Networks[C]//NDSS. 2009.

[9] Blondel V D, Guillaume J L, Lambiotte R, et al. Fast unfolding of communities in large networks[J]. Journal of Statistical Mechanics: Theory and Experiment, 2008, 2008(10): P10008.

[10] Richardson M, Domingos P. Mining knowledge-sharing sites for viral marketing[C]//Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2002: 61-70.

[11] Domingos P, Richardson M. Mining the network value of customers[C]//Proceedings of the seventh ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2001: 57-66.

[12] Kempe D, Kleinberg J, Tardos . Maximizing the spread of influence through a social network[C]//Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2003: 137-146.

[13] Kempe D, Kleinberg J, Tardos . Influential nodes in a diffusion model for social networks[M]//Automata, languages and programming. Springer Berlin Heidelberg, 2005: 1127-1138.

[14] Chen W, Wang C, Wang Y. Scalable influence maximization for prevalent viral marketing in large-scale social networks[C]//Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2010: 1029-1038.

[15] Milgram S. The small world problem[J]. Psychology today, 1967, 2(1): 60-67.

[16] Nagaraja S. Anonymity in the wild: Mixes on unstructured networks[C]//Privacy Enhancing Technologies. Springer Berlin Heidelberg, 2007: 254-271.

[17] Wei W, Xu F, Tan C C, et al. Sybildefender: Defend against Sybil attacks in large social networks[C]//INFOCOM, 2012 Proceedings IEEE. IEEE, 2012: 1951-1959.

[18] Hastings W K. Monte Carlo sampling methods using Markov chains and their applications[J]. Biometrika, 1970, 57(1): 97-109.