A SURVEY ON SYBIL ATTACKS IN SOCIAL NETWORKS

M.SHAHIRA BANU, S.LAKSHMI NARASIMMAN
Information Technology, IFET College of engineering, Villupuram, India
Assistant Professor, Information Technology, IFET College of engineering, Villupuram, India

ABSTRACT
The Sybil attack is an attack wherein a reputation system is subverted by a considerable number of forging identities in peer-to-peer networks. Most peer-to-peer systems are vulnerable to Sybil attacks. By illegitimately infusing false or biased information via the pseudonymous identities, an adversary can mislead a system into making decisions benefiting herself. Sybil attacks can be avoided by using trusted certification. Trusted certification usually relies on a centralized trusted authority for assigning and verifying identities. Sybil accounts in online social networks are used for criminal activities such as spreading spam or malware stealing other users’ private information and manipulating web search results. Preventing Sybil attacks is quite challenging. In this paper we summarize the existing methodologies used to detect and prevent the Sybil attacks in social networks.

Keywords-forging, identities, peer-to-peer networks, Sybil attack, vulnerable

1. INTRODUCTION
A Sybil attack [1] is one in which a malicious node on a network illegitimately claims to be several different nodes simultaneously. Many distributed applications and everyday services assume each participating entity controls exactly one identity. When this assumption is unverifiable the service is subject to attack. In a Sybil attack, an adversary creates a large number of false/fake/Duplicate identities (Sybil identities), and since all Sybil identities are controlled by the adversary. It can maliciously introduce a considerable number of false opinions into the system, and convert it, by making decisions benefiting system itself. To defend against the attack, there have been several attempts in the form of defenses, or mitigations, to defend against, or limit, the impact of the attack. Such attempts can be classified broadly into two schools of thoughts: centralized and decentralized (i.e., distributed) defenses. In centralized defenses [2-5], a centralized authority is responsible for verifying the identity of each and every user in the system. While this defense is somewhat effective in defending against the attack, it makes certain assumptions about the system, some of which are not easy to achieve in peer-to-peer decentralized systems. First of all, as the name and description implies, such systems require a centralized authority, which might not be affordable for both security and functionality reasons. Even if such a centralized authority exists, it requires credentials for users in the system to match against each user’s digital identity. On the other hand, many decentralized defenses [6-16] do not require such authorities and are well designed for decentralized peer-to-peer systems. At the core of their operation, such defenses weigh collaboration among users in the system to admit or reject users who are potential attackers. Admission or rejection of users is based on credentials associated with them, as in the case of cryptographic distributed defenses, or network properties of legitimate, honest users, as in the case of Sybil defenses using social graphs. In either of these solutions, the ultimate goal of the defense is to simulate the power of the centralized authority in a decentralized manner and use such power to detect both Sybil and honest nodes. The number of fake identities that can be injected into the system formally characterizes the attacker. The attacker’s objective is to maximize this number. The value and meaning of the number of identities generated by the attacker and injected into the system depends on the application itself and varies from application to application. For better understanding we provide some of the mechanisms used for the detection of Sybil nodes.

1.1 SYBILGUARD
The SybilGuard design from Yu et al. [14, 15] uses the fast mixing property of trust-possessing social networks to detect Sybil nodes. Technically, SybilGuard consists of two phases: initialization and online detection. In the initialization phase, each node constructs its routing table as a random permutation of its adjacent nodes for pairs of incoming and outgoing edges. Next, each node initiates a random walk of length \( w = O(n \log n) \) and propagates it to its adjacent nodes following the routing tables constructed using the random permutation. Each node on the path of the random walk publicly registers the random walk originator and later acts as a witness for that node if that node becomes suspect. Furthermore, using back-traceability of the random walks, each originator of a random walk receives the list of witnesses (i.e., the nodes that registered the originator’s public key and that lie on the path constructed by the random walk

www.ijsret.org
of the originator). In the online phase, a verifier determines whether a suspect is honest or not. First, the suspect sends the addresses of the witnesses on its random route to the verifier. Accordingly, the verifier compares the list of witness to its list of the verifier route. If there is no intersection between the two sets (an event with a very low probability) the verifier aborts and rejects the node. Otherwise, the verifier continues by contacting the nodes on the intersection between the two sets to verify if the suspect has a public key registered with them. If the intersection nodes verify the suspect, the verifier accepts the node; otherwise, it marks it as a Sybil node.

### 1.2 SYBILLIMIT

Unlike SybilGuard in which a single long random walk is used, SybilLimit [13] suggests the use of several shorter random walks. Also, unlike SybilGuard where public keys of verifiers and suspects are registered on nodes in the social graph, SybilLimit suggests the registration of such keys on edges in the social graphs. SybilLimit consists of an initialization phase and an online verification phase. In the initialization phase, each node constructs its routing table using the same method described in SybilGuard and performs $r=O(\sqrt{n})$ random walks, each of length $w=O(\log n)$ where $O(\log n)$ is the mixing time of the social graph, which is 10 to 15 in a million-node social graph, and is theoretically assumed to be a sufficient sample from a distribution that is very close to the statistical distribution. Unlike SybilGuard, where all nodes on the path of the random route are used for registering the public key of the originator of the random walk, the last edge in each walk among the $r$ random walks is used for registering the public key of that originator node (each such edge is called a tail). In particular, the public key of the originator of the walk is registered at the last node in the walk under the last edge through which the random walk arrived. In addition, using the back-traceability property of the random routes, the witnesses that register the public key of the originator node (which could be either a suspect or a verifier) return their identities to that node. Every node in the social graph performs the same process, and collects sets of witnesses (or verification nodes).

In the online phase, as with SybilGuard, the suspect sends the identifiers and addresses of the witnesses to the verifier node, which compares the witnesses in the suspect's list trying to find a match. If a match is found in the two sets by the verifier, it asks a witness with common identity in both sets to verify the identity of the suspect node and decides whether to accept or reject the node based on the outcome of this process. If no intersection happens between the two sets (a very low probability) the verifier aborts and rejects the node, labeling it an attacker. The main ingredients used for reasoning out the provable guarantees of SybilLimit are same as those in SybilGuard. In particular, given that the random walk length $w$ is the mixing time of the social graph, the last node selected in such a random walk is found according to the stationary distribution. Furthermore, the last edge in the random walk is selected almost uniformly at random from the edges in the social graph. In addition, given that $r=O(\sqrt{n})$, an intersection between the sampled edges of the verifier and the suspect exists with overwhelming probability if the hidden constant $r_0$ (where $r_0=\Omega(\sqrt{n})$) is chosen correctly. The authors refer to this condition as the intersection condition, which is used to ensure a high probability for intersection of random walks by honest nodes. As in SybilGuard, assuming $g$ attacker edges, the attacker is allowed to register public keys of Sybil identities on at most $g\times w\times r_0 = O(g\sqrt{n}\log n)$ tails (called tainted tails). In such cases, each attached edge introduces additional $O(\log n)$ Sybil identities (assuming that the attacker uses the optimal attack strategy by registering different public keys of different Sybil identities with each possible tainted tail). SybilLimit also greatly depends on $w$ for its security. Since there is no mechanism for estimating the exact value of the parameter, underestimating or overestimating such a parameter are both problematic, as shown above. SybilLimit also provides a benchmarking technique for estimating this parameter, which does not provide a guarantee of the quality of the estimation of the parameter. Finally, SybilLimit can provide guarantees on the number of Sybil identities introduced per attack edge as long as $g=\omega(n/\log n)$. Notice that both SybilGuard and SybilLimit do not require global knowledge of the social network they operate on, and can be implemented in a fully decentralized manner.

### 1.3 SYBILLIFIER

SybilInfer [17] uses a probabilistic model defined over random walks (called traces) in order to infer the extent to which a set of nodes, $X$, which generated such traces, is honest. The basic assumptions in SybilInfer are that each node has a global view and knowledge of the social network, the network is fast mixing, and the node that initiates SybilInfer is an honest node. Technically, SybilInfer tries to ultimately label the various nodes in the graph into honest or Sybil nodes. In SybilInfer, each node in a network of $n$ nodes performs $s$ walks; hence, the overall number of walks in the universal trace is $s\times n$. Each trace among these traces consists of the first node (the initiator of the random walk) and the last node in the random walk (i.e., the tail). Unlike the uniform (over node degree) transition probability used in SybilGuard and SybilLimit, SybilInfer defines the transition matrix...
uniform over nodes, thus penalizing nodes with a higher degree. The ultimate goal of the operation of SybilInfer is to compute probability \( P(X=\text{Honest}|T) \), that is, compute the probability that a set of nodes \( X \) is honest, given the traces, \( T \). This probability is computed using Bayes’ theorem. SybilInfer also uses non-trivial techniques for sampling the honest configuration that is used initially to determine the honesty of a set of nodes from their traces. This sampling is performed using the Metropolis-Hasting algorithm by initially considering a set \( X_0 \) and modifying the set by either removing or adding nodes to the set. Each time, with probability \( \text{Padd} \), a new node \( x \) from \( X_0 \) is added to \( X_0 \) to make \( X'=X_0vx \), or a node in \( X_0 \) is removed with probability \( \text{Premove} \). The process is performed for \( n \log n \) rounds in order to obtain a good sample independent of \( X_0 \).

2. LITERATURE SURVEY

In this section, we propose a survey about how to detect and prevent the Sybil attacks and the mechanisms. [18] Describes the SybilGuard, a novel protocol for limiting the corruptive influences of Sybil attacks. This protocol is based on the “social network” among user identities, where an edge between two identities indicates a human established trust relationship. Malicious users can create many identities but few trust relationships. Thus, there is a disproportionately small “cut” in the graph between the sybil nodes and the honest nodes. SybilGuard exploits this property to bound the number of identities a malicious user can create. Sybil Guard guarantees that an honest node accepts, and also is accepted by, most other honest nodes with high probability. Thus, an honest node can successfully obtain service from, and provide service to, most other honest nodes. SybilGuard also guarantees that with high probability, an honest node only accepts a bounded number of Sybil nodes. SybilGuard leverages the existing human-established trust relationships among users to bound both the number and size of Sybil groups. All honest nodes and sybil nodes in the system form a social network. An undirected edge exists between two nodes if the two corresponding users have strong social connections (e.g., colleagues or relatives) and trust each other not to launch a Sybil attack. If two nodes are connected by an edge, we say the two users are friends. Here the edge indicates strong trust, and the notion of friends is quite different from friends in other systems such as online chat rooms. An edge may exist between a Sybil node and an honest node if a malicious user (Malory) successfully fools an honest user (Alice) into trusting her. Such an edge is called an attack edge and the authentication mechanism in SybilGuard ensures that regardless of the number of Sybil nodes. [19] Describes the Sybil defense to detect local communities (i.e., clusters of nodes more tightly knit than the rest of the graph) around a trusted node. Malicious attackers can create multiple identities and influence the working of systems that rely upon open membership. All social network-based Sybil defense schemes make the assumption that, although an attacker can create arbitrary Sybil identities in social networks, he or she cannot establish an arbitrarily large number of social connections to non-Sybil nodes. As a result, Sybil nodes tend to be poorly connected to the rest of the network, compared to the non-Sybil nodes. Sybil defense schemes leverage this observation to identify Sybils. [20] Describes an empirical analysis of the cyber criminal ecosystem on Twitter. Essentially, through analyzing inner social relationships in the criminal account community, criminal accounts tend to be socially connected, forming a small-world network. Also finding the criminal hubs, sitting in the center of the social graph, are more inclined to follow criminal accounts. Through analyzing outer social relationships between criminal accounts and their social friends outside the criminal account community, revealing three categories of accounts that have close friendships with criminal accounts. Cyber criminals have utilized Twitter as a new platform to conduct their malicious behavior including sending spam and phishing scams [23], spreading malware [24,25], hosting botnet command and control (C&C) channels [26], and launching other underground illicit activities. Analyze inner social relationships in the criminal account community to reveal insights on how criminal accounts socially connect with each other. Meanwhile, we analyze outer social relationships between criminal accounts and their criminal supporters to reveal the characteristics of those accounts who have close friendships with criminal accounts. Finding possible reasons why criminal supporters outside the criminal community become criminal accounts’ followers. Essentially, these supporters aid criminal accounts in avoiding detection by increasing criminal accounts’ followers, and in preying on more victims due to the “social-intercourse” nature of Twitter (Twitter users may visit their friends’ friends’ profiles). Through these analyses, understanding how the criminal accounts mix into the whole Twitter space, and presenting new defense insights to effectively catch Twitter criminal accounts. Social Butterflies are those accounts that have extraordinarily large numbers of followers and followings. Like social butterflies in our real life, these accounts build a lot of social relationships with other accounts without discriminating those accounts’ qualities. Dummies are those Twitter accounts who post few tweets but have many followers. Since in Twitter, legitimate users tend to follow those accounts that share more useful information, it is relatively weird that these dummies has close relationships with criminal accounts.
while sharing little information, but they have many followers.[21] Describes the Online social networks have become extremely popular; numerous sites allow users to interact and share content using social links. Users of these networks often establish hundreds to even thousands of social links with other users. Social networking sites allow only a binary state of friendship; it has been unsurprisingly observed that not all links are created equal. A recent study [25] has demonstrated that the” strength of ties “varies widely, ranging from pairs of users who are best friends to pairs of users who even wished they weren’t friends. In order to distinguish between these strong and weak links, researchers have suggested examining the activity network, the network that is formed by users who actually interact using one or many of the methods provided by the social networking site. Evolution of activity between users at both the microscopic and macroscopic levels. At the microscopic level, we investigate how pairs of users in a social network interact, and at the macroscopic level, we examine how the varying patterns of interaction affect the overall structure of the activity network. Characterizing the patterns of interaction between pairs of users in Facebook. Observing a strong skew in the total number of wall posts exchanged between user pairs; a majority of the user pairs display very little activity, but a minority is highly active. To better understand the patterns of both active and relatively inactive relationships, separating the user pairs into two groups and examining their interaction patterns in detail. The low-level interaction group typically takes more than a month to initiate their wall interaction since the time they become friends.

3. CONCLUSION
Peer-to-peer systems play an ever-increasingly important part of our daily lives. In order to prevent the sybil attacks first we provided the mechanisms used to detect the Sybil, second the approaches used to identify the bending from sybil nodes. In this paper we review the different way to identify the fake/sybil/false accounts in online social networks.

REFERENCES
[8] F. Lesueur, L. Me, V. V. T. Tong, —A Sybil-resistant admission control coupling Sybilguard with distributed certification,l in Proc. of WETICE, Washington, DC, USA, pp. 105-110, 2008. Article (CrossRef Link)
[16] N. Tran, J. Li, L. Subramanian, S. S. Chow, —Optimal sybil-resilient node admission control,l in


AUTHORS BIOGRAPHY

Ms. M. SHAHIRA BANU currently pursuing B.Tech. Information Technology at IFET College of Engineering, Villupuram, India. Her area of interests includes OOPS concepts, Cryptography and Data mining and networking. Email: shahiranisha@gmail.com

Mr. S. Lakshmi Narasimman completed B.Tech Information Technology from Anna University, Chennai and completed M.Tech in CSE from Bharath University. Interested in computer networks, formal languages and data mining. Email: narasimman0388@gmail.com