Research Paper
Volume : 5 | Issue : 8 | Special Issue August-2016 • ISSN No 2277 - 8179

TrustFriends: A Trustworthy Social Network by Sybil Defense and Compromised Account Detection

Engineering

KEYWORDS: Sybil Attack, Online Social Network, Sybil community, Victims, Customers.

Fahida V P	PG Scholar, Computer Science and Engineering Vedavyasa Institute of Technology
Ginnu George	Asst.Professor, Computer Science and Engineering Vedavyasa Institute of Technology

ABSTRACT

Sybil attack is a fundamental problem in the area of online social network. Several methods have been proposed in the literature to detect Sybils. But none of the methods considers the case of attackers who are buying friends from miscreants, a growing industry that have emerged to help social network users create a large network of friends. These websites promises their subscribers to provide friends for sale, free or paid. Thus Sybils can befriend a large number of real users by subscribing services provided by these online friend markets. No existing detection technique can detect Sybil, with many real users as friends.
This paper proposes a new technique called TrustFriends, a system which integrates Sybil detection and market user detection. Sybil detection is based on a friend invitation graph, which is a signed directed graph, models friend invitation interactions. It consist of two phases, Individual Sybil detection and Sybil Community detection. Market user detection also have two key mechanisms, Victim detection to find free market service subscribers and Customer detection to find paid subscribers.

I. INTRODUCTION

One of the prevalent and practical attack against Online Social Network (OSN) is Sybil attack[1], a malicious user creates multiple fake identities called Sybils [1] to unfairly increase their power and influence within a target community. There are several techniques have been proposed in the literature to detect fake identities [2] – [7]. But none of them distinguish between Sybil and Compromised accounts. A compromised account is one whose login credentials will be obtained by a third party. An account can be compromised in a number of ways, by using a phishing scam to steal the user's credentials or by logging into some websiteswith same credentials.

To address the problem of Sybil attacks in OSNs, many Sybil defense schemes have been proposed in the literature [1] - [7]. These existing defenses rely on the assumption that Sybil could befriend only few real users. Thus those schemes consider only positive trust relationship among users and models OSN as a social graph structure. But later researches shows that real users in OSN have a non-zero probability of accepting friend request from strangers. Thus Sybils can add many real users as friends by sending large number of friend requests, which invalidates the assumption behind social graph structure. Another defense scheme [11] which uses friend invitation graph to model OSNs overcome the limitations associated with social graph structure. Friend Invitation graph consider both positive trust relationship in the form of accepted friend requests and negative distrust relationship in the form of rejected friend requests.

Recent works [12], have found that attackers are buying friends from miscreants, a growing industry that have emerged to help social network users create a large network of friends. For Example, Twitter Follower Markets [12]. In this paper the term Online Friend Market (OFB) is used in general to denote miscreants. OFB is a website which provides friends for sale, free or paid. Some markets uses fake accounts to boost the count of friends, while others rely on pyramid scheme to turn non-paying customers to add friends for each other and into paying customers. The existence of such markets may cause the count of real friends for a Sybil account to grow. Because many real users also approaches OFBs to boost the count of their friends as well as Sybils.

A Sybil with many real friends cannot be categorized as a Sybil. Thus to overcome this problem, a technique to detect market users is required. This paper aims to extend earlier techniqueVoteTrust [11] by integrating market user detection along with it. VoteTrust is a Sybil detection scheme and it is not enough to detect all fake identities in an OSN. Because online markets provides many real friends to the market service subscribed Sybils, then it behave like real user and cannot be categorized as Sybil. Thus in addition to Sybil detection in OSNs, Online market user detection will be required to detect whole fake identities from OSNs. Market users are classified as Victims and Customers. Those who subscribed free service are called Victims and those who subscribed paid service are called Customers.

Online social network is very popular for last few years. The large use of these social network has attracted the attention of cyber-criminals. To address the problem of malicious activities on OSN, researchers have started to propose different detection and mitigation approaches. Initial work has focused on the detection of fake accounts (i.e., automatically created accounts with the sole purpose of spreading malicious content). Unfortunately, systems that detect fake accounts do not discriminate between Sybil and compromised accounts. A compromised account is an existing, legitimate account that has been taken over by an attacker. Accounts can be compromised in a number of ways, for example, there are some online markets for buying friends by compromising account. In this paper, a novel approach to detect compromised accounts on social networks is proposed. By identifyingcompromised accounts, social network providers can focus their mitigation efforts on real users.

This paper is organizes as follows. In Section II various literature papers have presented. Section III discusses about VoteTrust, a Sybil defense scheme and its limitation. In Section III and IV a method to overcome the limitation is presented. Section V analyses the result and Section VI draws conclusion.

II. LITERATURE SURVEY

A. SybilGuard

To prevent Sybil attacks, SybilGuard [2] performs the random walks over constrained random routes. Random route require each node to use a pre-computed random permutation as a one-to-one mapping from incoming edges to outgoing edges giving them the following important properties: Convergence, two routes traverse the same edge along the same direction, they will merge and stay merged and Back-traceability, the outgoing edge of a random route uniquely determines the incoming edge at an honest node.

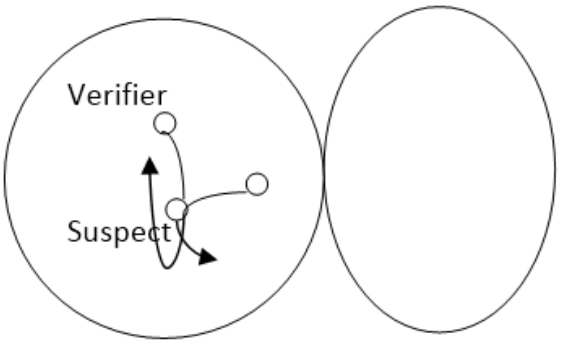

Fig.1. The verifier's random route accepts the suspect because the random routes intersect.

The validation criterion for accepting a node as honest in SybilGuard is that there should be an intersection among the random route of the verifier node and suspect node as shown in Fig.1.

SybilGuard's security depends upon the number of attack edges, connecting honest and Sybil nodes. To intersect a verifier's random route, a Sybil node must traverse an attack edge (say X). The random routes of all Sybil nodes traversing along X will intersects verifier's random route at the same node and along the same edge, due to convergence property. All such nodes form an equivalence group, thus the number of Sybil group is bounded by the number of attack edges.

B. SybilLimit

Instead of using a single instance of very long random routes, SybilLimit [3] employs multiple instances of short random walks to sample nodes from the honest sets. The number of Sybil nodes accepted is reduced around 200 times in the experiments for a million-node system, as compared to SybilGuard [2]. This is because a short random walk is likely to stay within the set of honest nodes.

SybilLimit has two component protocols: a secure random route protocol and a verification protocol. The first protocol runs in the background and maintains information used by the second protocol.

Secure random route protocol: In the protocol, each node has a public/private key pair and communicates onlywith its neighbors in the social network. Every pair of neighbors share a unique symmetric secret key called the edge key for authenticating each other. A suspect starts a random route along a uniformly random edge and propagates along the route its public key Ks together with a counter initialized to 1. Every node along the route increments the counter and forwards the message until the counter reaches ω, the length of a random route.

Verification protocol: A verifier V invokes this protocol to determine whether to accept a suspect node. A suspect node S must satisfy both intersection condition and balance condition to be accepted. Intersection condition requires that S's tails and V's tails must intersect, with S being registered at the intersecting tail. In contrast, SybilGuard has an intersection condition on nodes instead of on edges or tails. For the Balance condition V maintains counters corresponding to its r tails. Every accepted suspect increments the "load" of some tail. The balance condition requires that accepting S should not result in a large "load spike". In comparison, SybilGuard does not have any balance condition.

C. SybilDefender

SybilDefender [4] can detect a Sybil region at a time instead of a single Sybil node. SybilDefender consist of three components: Sybil identification algorithm, Sybil community detection algorithm and two approaches to limiting the number of attack edges. The three components can be used in conjunction to best mitigate Sybil attacks.

Sybil Identification algorithm: The intuition of Sybil identification algorithm is that, as there is a small cut between the honest region and the Sybil region, the random walks originating from a Sybil node tend to get "trapped" into the Sybil region. Also, since the assumption that the size of the Sybil region is not comparable to the size of the honest region, the number of nodes traversed by the random walks originating from an honest node will be larger than the number of nodes traversed by the random walks originating from a Sybil node, as long as the random walks are long enough and perform the random walks many times. For simplicity, define the number of times one node being traversed by a set of random walks as the frequencyof that node. Note that one node may be traversed by the same random walk multiple times. Then nodes whose frequency is less than a threshold will be detected as Sybil.

Sybil community detection algorithm: After one Sybil node is identified, our Sybil community detection algorithm can be used to detect the Sybil community surrounding it.The Sybil community detection algorithm takes social graph G (V,E) and a known Sybil node as 'S' input and output Sybil community around S.

Limiting the number of attack edges: It has been shown that not all the relationships in online social networks are trusted. One approach to limiting the number of attack edges in these networks is to allow the users to rate their relationships. That is users of the OSN can rate each of their relations either as "Friend" or "Stranger", where "Stranger" means the user hardly has any impression about this relation. The number of attack edges can be limited by removing the relationships rated as stranger from the social graph when applying the Sybil defense schemes. The rationale is that even if an adversary can create many links between the Sybil identities and the honest identities, it is hard for him to convince the honest users that those Sybil identities are their acquaintances.

D. SybilInfer

SybilInfer [5] is another algorithm for labelling nodes as honest or Sybil. At the heart of SybilInfer lies a probabilistic model of honest social network, and an inference engine that returns potential regions of Sybil nodes. The Bayesian inference to Sybil detection comes with the advantage label has an assigned probability, indicating its degree of certainty.

The SybilInfer algorithm takes a social graph G and a single known trusted node that is part of this graph as its input and performs the following steps. Finally, returns the probability that each node is honest or Sybil.

- A set of traces T are generated and stored by performing special random walk over social graph G.
- A probabilistic model is then defined that describe the likelihood a trace T was generated by a specific set of honest nodes within G, called X. Given the probabilistic model, the trace T and the set of honest nodes we can calculate Pr[T|X is honest].
- Once the probabilistic model is defined, Bayes theorem can be used to calculate, for any set of nodes X and the generated trace T, the probability that X consist of honest nodes. Mathematically it is represented as Pr[X is honest|T].
- Since it is not possible to simply enumerate all subsets of nodes X of the graph G, we instead sample from the distribution of honest node set X, to only get a few $X_0,\ldots,X_N \sim$ Pr[X is honest|T]. Using those representative sample set of honest nodes, we can calculate the probability any node in the system is honest or Sybil.

Its applicability and performance is a little bit better than previous systems like SybilGuard and SybilLimit. The key difficulty of this approach is the definition of probabilistic model over the traces T, and its inversion using Bayes theorem to define a probability distribution over all possible set of honest nodes X.

E. SumUp

Collecting user votes is essential to ranking the user generate online contents. For Example, YouTube videos are ranked according to user ratings. This kind of voting system is easily Susceptible to Sybil attacks where adversaries can out-vote real users by creating many Sybil identities. SumUp [6], a Sybil resilient content vote aggregation system uses the technique of adaptive vote flow aggregation to limit the number of bogus votes cast by adversaries to not more than the attack edges in the network.

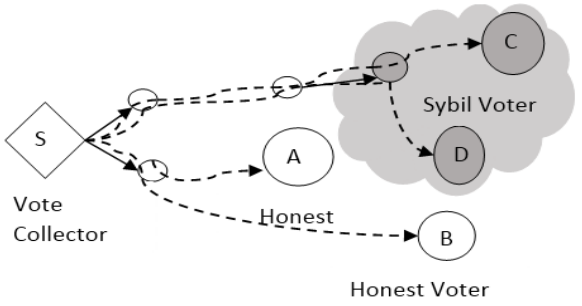

Fig.2.SumUp computes a set of approximate max-flow paths from the vote collector s to all voters (A, B, C, D).

Here SumUp is described in a centralized setup where a trusted central authority maintains all the information in the system. SumUp aggregates votes from one or more trusted vote collectors. SumUp can operate in two modes, personalized vote aggregation and global vote aggregation. In personalized vote aggregation each user has its own vote collector to collect the votes of others. As each user collects different number of votes on same object, he also has a different ranking of content. In global vote aggregation, one or more pre-selected vote collectors are used to collect votes on behalf of all users. Global vote aggregation has the advantage of allowing for a single global ranking of all objects.

In a trust network any node either an honest or a Sybil can cast a vote on any object to express his opinion. Each vote is either positive or negative i.e.; +1 or -1. To make a vote more expressive, its value can vary within a range with higher values indicating more favorable opinions. Voting system also let the vote collector provide negative feedback on malicious votes. In personalized vote aggregation, each collector gives feedback according to his personal taste. In global vote aggregation, the vote collector should only provide objective feedback, e.g. negative feedback for positive votes on corrupted files.

SumUp computes a set of max-flow paths in the trust graph from the vote collector to all voters on a given object, in order to limit the number of votes that Sybil identities can propagate for an object. Fig.2 shows max-flow calculation from collector to voters. Each vote flow consumes one unit of capacity on each link traversed.

F. SybilControl

The goal of SybilControl [7] is not to completely prevent adversaries from joining the system, but rather to place a limit on the number of additional Sybil nodes adversaries can join. This prevents them from obtaining significant influence over the system. SybilControl operates towards this goal using the following insight: if a computational cost is incurred by nodes before they are allowed to join the system, then adversaries with finite resources will have an upper bound on the rate they can acquire identities. Moreover, if nodes are required to periodically repay this computational cost to retain their identities, then the number of identities that can be maintained by the adversary will be limited. To leverage this insight, SybilControl uses computational puzzles to control admission and retainment of nodes in a system. It provides a distributed protocol that allows nodes to collectively verify that their neighbors are paying computational costs. Then in this environment, it provides enforcement mechanisms that eliminate the influence of misbehaving nodes that do not solve puzzles.

In Fig.3, Node A maintains a puzzle solution $S_{A\,old}$ and its associated challenge $C_{A old}$. Node a receives Challenges C from node B1, B2 and B3, which are used along with A's old challenge to periodically compute a new challenge $C_{A\,new}$. Node A periodically generates a fresh puzzle solution based on its new challenge.Before a node A trusts communication with another node B, A requires B to prove that it recently solved a puzzle. If B is a malicious Sybil node and chooses not to solve the puzzles, it will not be able to provide proof of work.Defense mechanisms in SybilControl protect honest nodes like A from using B, essentially making B non-functional in the system and preventing it from doing harm. This forces adversaries to use only puzzle-solving Sybils, of which they can support a limited number.

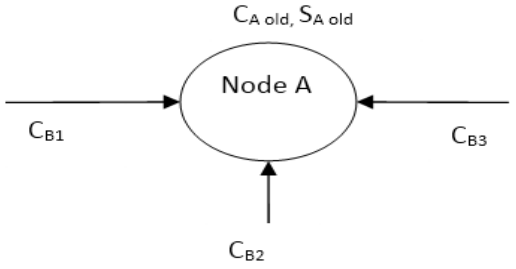

Fig.3. Overview of SybilControl

G. SybilRank

It relies on social graph properties to rank users according to their perceived likelihood of being fake (Sybils). SybilRank [8] operates in three stages. In stage 1, trust flows from known non-Sybil nodes (trust seed) and spread over the entire network with a bias towards the non-Sybil region. In stage 2, SybilRank ranks nodes based on their degree-normalized trust. In the final stage, SybilRank assigns a portions of fake nodes in the intervals of the ranked list.

Propagating trust: Power iteration involves successive matrix multiplications where each element of the matrix represents the random walk transition probability from one node to a neighbor node. Each iteration computes the landing probability distribution over all nodes as the random walk proceeds by one step.

Ranking by degree-normalized trust: Ranking nodes by degree-normalized trust for the following two reasons. Eliminating node degree bias, this design gives each non-Sybil node almost identical degree-normalized trust. It reduces false positives from low degree non-Sybil nodes and false negatives from high-degree Sybils.

Annotating the ranked list: SybilRank relies on the limited attack edges to distinguish Sybils. It may give high rankings to the Sybils that obtain many social links to non-Sybil users, and consider them as non-Sybil users. This is true for all social-graph based defenses. It may result in even the top and bottom intervals of the ranked list to comprise a non-negligible portion of fake and real accounts, respectively. Thus, an OSN cannot simply identify a pivot in the ranked list below which all nodes are fake, and it still has to rely on manual inspection.

H. TrustRank

TrustRank [9] seeks to combat spam by filtering the web based upon reliability. The method calls for selecting a small set of seed pages to be evaluated by an expert. Once the reputable seed pages are manually identified, a crawl extending outward from the seed set seeks out similarly reliable and trustworthy pages. TrustRank's reliability diminishes with increased distance between documents and the seed set.

The algorithm is based on a semi-automatically technique. The basic idea of Trust Rank algorithm is that a link between two nodes on the web signifies trust between them. The Trust of two nodes can be propagated through the link structure on the Web. So, a list of highly trustworthy nodes are selected to form the seed set and each of these node is assigned a non-zero initial trust score, while all the other nodes on the Web have initial values of 0. A biased PageRank algorithm is then used to propagate these trust scores to their descendants. After convergence, good node will have relatively high trust scores, while spam node will have poor trust scores. For example, if more computers pages exist in the seed set than pages related to sports, then pages related to computers have a better chance of gaining higher trust scores than the pages related to sports.

I. BadRank

BadRank [10] is a method for detecting spam web sites, based on the premise that a page is spam if it points to another spam page; i.e., the BadRank score of a page is the weighted sum of the BadRank scores of the pages that it links to. BadRank is an important tool in spam detection. Consider the mathematical structure of BadRank, showing how it can be modified to guarantee that iterates converge. Additionally, consider methods for incorporating knowledge about trusted (known non-spam) sites into the BadRank calculation by changing the underlying iteration matrix. The difference between TrustRank and BadRank is that first one selects a trusted node and assign a trust score, but late one selects a bad node and assigns a bad score.

III. VOTETRUST: FRIEND INVITATION GRAPH BASED SYBIL DEFENSE SCHEME

VoteTrust, is a voting based Sybil detection scheme and it uses friend invitation graph to model interaction among OSN users. Friend Invitation graph is a signed directed graph. Each node represents a user and the edge is directed from sender to receiver. The sign on edge may be +1 or -1, depending up on whether the request is accepted or not as shown in Fig.4.In VoteTrust each node has two properties:

Vote Capacity $\vartheta(u)$ is the number of votes that v can cast on another node. Given a link (u, v, s) in G, it means that node v casts at most $\vartheta(v)$ votes on node u, and the vote value $x_{vu} = s(+1 \text{ or } -1)$

Global Acceptance Rate $p(u)$is the fraction of positive votes that VoteTrust aggregates for a node u, indicating the probability that u is accepted by real users. Nodes with low global acceptance rate (e.g., below a certain threshold δ_f) are detected as Sybils.

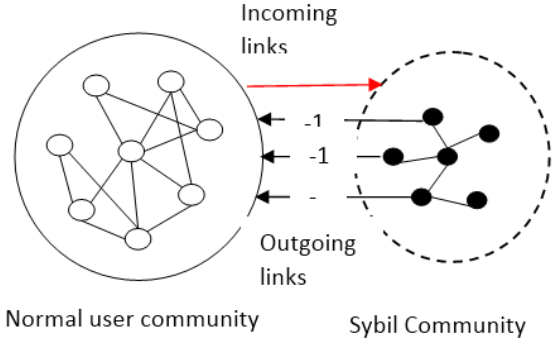

Fig.4. Illustration of friend invitation graph

VoteTrust detects Sybil through two phases, Individual Sybil detection and Sybil Community detection. First phase consist of two steps, Vote assignment and Vote aggregation. A node with $p(u) < \delta_f$ is detected as Sybils, where δ_f is detection threshold.Individual Sybil detection algorithm is shown in Fig.5.

After Individual Sybil detection second phase to setect Sybil Community is performed, which detects Sybils surrounding the individual Sybils detected in previous phase. Sybil Community detection algorithm is shown in Fig.6

Here first select a bad seed and assign a bad score. Then propagate bad score to other nodes also. After that select nodes with high bad score in order to expand Sybil community. Some real users could also have relatively high bad score due to unintentionally sending friend request to Sybils. Thus Pruning real user step performs and remove such nodes from Community.

Recent researches [12] have found that miscreants start to sell legitimate account through some websites. Twitter Follower Market [12] is an example for such market. Thus, if Sybils are willing to buy friends from miscreants, they looks like Real user with many real friends and then they can enhance the attack capacity. In this case, VoteTrust can be considered as a first level defense mechanism and could be combined with other orthogonal techniques for even better defense.

1. **procedure** VoteTrust-D(G, V_s)
2. **if** u ∈ V_s **then** ↔**Vote assignment**
3. **I**(u) ← N/|V |;
4. **else**
5. **I**(u) ← 0;
6. **end if**
7. **while** Δ> ε_1 **do**
8. **for** u ∈ V **do**
9. $\vartheta(u) = d \cdot \sum_{v:(u,v)\in E} \frac{\vartheta(v)}{\omega(v)} + (1-d) \cdot$ **I**(u)
10. **end for**
11. **end while**
12. $p^{(0)} \leftarrow 0.5$; ↔**Vote aggregating**
13. **while** Δ> ε_2 **do**
14. **for** u ∈ V **do**
15. $p^{\wedge}(u) = \frac{\sum_{v:(v,u)\in E} \vartheta(v)p(v)}{\sum_{v:(v,u)\in E} \vartheta(v)p(v)}$
16. p ← WilsonScore($p^{\wedge}$);
17. **end for**
18. **end while**
19. **end procedure**

Fig.5. VoteTrust: Individual Sybil Detection algorithm

IV. TRUSTFRIENDS: EXTENDING VOTETRUST

The proposed methodology focuses on detecting compromised accounts in addition to Sybils. The main aim of this approach is to enhance the VoteTrust by integrating it with compromised account detection. As social networking sites have risen in popularity, cyber-criminals started to exploit these sites to spread malware and to carry out scams. Previous work has extensively studied the use of fake accounts that attackers set up to distribute spam messages, mostly messages that contain links to scam pages. Fake accounts typically exhibit highly anomalous behavior, and hence, are relatively easy to detect. As a response, attackers have started to compromise and abuse legitimate accounts. Compromising legitimate accounts is very effective, as attackers can leverage the trust relationships that the account owners have established in the past. Moreover, compromisedaccounts are more difficult to clean up because a social network provider cannot simply delete the corresponding profiles.

Thus a novel approach is required to detect compromised user accounts in social networks. Malicious accounts are easier to create, compromised accounts are more valuable to cybercriminals. The reason is that these accounts allow attackers to leverage the associated account history and network of trust to spread malicious content more effectively. As a result, attackers increasingly abuse legitimate accounts to distribute their malicious messages. To identify campaigns that involve both compromised and fake

Volume : 5 | Issue : 8 | Special Issue August-2016 • ISSN No 2277 - 8179

accounts, the focus of the analysis has shifted to the messages themselves. In particular, researchers have proposed techniques that search a social network for the presence of similar messages. The intuition is that attackers send many similar messages as part of campaigns. Similarity is typically defined in terms of overlap in message content or shared URLs.

1. **procedure** VoteTrust-C(G,V_s)
2. **if** u ∈ V_s **then** ↔**Bad score propagation**
3. I(u) ← 1
4. **else**
5. I(u) ← 0;
6. **end if**
7. **while** Δ> ε_1 **do**
8. **for** u ∈ V **do**
9. $B(u) = d \cdot \sum_{v:(u,v)\in E} \frac{B(v)}{\varphi(v)} + (1-d) \cdot I(u)$
10. **end for**
11. **end while**
12. $C_0 \leftarrow V_s$; ↔ **Community expansion**
13. **Repeat**
14. C ← TopBadScoreNodes(2|C_0|);
15. **for** u ∈ C **do** ↔ **pruning real users**
16. **if** Ω(u) < 0 **then**
17. C = C – {u};
18. **end if**
19. **end for**
20. **for** u ∈ D **do** ↔ **Adding other Sybils**
21. **if** Ω(u) > 0 **then**
22. C = C ∪ {u};
23. **end if**
24. **end for**
25. $\Delta \leftarrow 1 - \frac{|C \cap 0|}{|C|}$
26. $C_0 \leftarrow$ C;
27. **until** $|C_0| > 0$ & Δ< ε_2
28. **end procedure**

Fig.6. VoteTrust: Sybil Community Detection algorithm

An account is considered as compromised if a third party has obtained access to that account (e.g., through a phishing attack or by tricking the user into authorizing an application) and uses this account in a way that violates OSN's terms of service. This includes, for example, posting unrelated updates on trending topics, or so-called mention spam where a large number of posts mention users that have no relation with the account that sends the posts. Unfortunately, many of these compromised accounts end up under the control of so-called online markets. These markets provide services that simplify building up influence in the social network by artificially inflating the number of friends and offering spam-like advertising services so-called promoted posts. However, the way these markets operate directly violates OSN's terms of service. Online Markets make use of compromised accounts for two different purposes: inflating friends and sending promoted posts.

Inflating Friends: Online Friend Markets uses compromised account credentials to befriend them each other. This may lead to increase in the friend's count of those victim accounts. The increased number of friends make the victim account more trustworthy and influential to other users. This is an advantage to Sybil accounts, because their fake profile looks like real with lots of real friends, who also compromise their account.

Promoted Posts: The Online Friend Markets uses the compromised account that they control to send posts arbitrarily. Those posts may include malicious contents or URLs points to their websites, in order to attract many other users towards such market. Companies and individuals need to promote their posts or to reach their product in a wide variety of audience and this is the main reason for the success of such market. It requires more time and effort to create a legitimate and functional network of friends for an account.Thus, Companies and individuals contacts this kind of online friend markets to buy friends, instead of growing their social circles over time. Commonly, these Online Markets advertise their services as being legitimate and in line with all applicable rules. This tricks victims into handing over their credentials. After getting victim's account credentials attackers can use victim account to send and receive friend requests, also to send promoted posts periodically.An approach to identify compromised accounts is thus integrated with VoteTrust.

The approach to detect Compromised accounts consist of two stages. First, identify the victim accounts that gave away their credentials when they subscribed to the market for free. Second, analyze the accounts these victims follow, which allows us to identify paying customers of the market.

A. Detecting Market Victims

Market victims periodically send advertisement posts. These posts aim at attracting new users and luring them into subscribing to the service. Such postscontain similar text, point to the same website, or contain the same hashtag (e.g., #newfollow), therefore which are easily recognizable.

To identify Online Friend Market from a given collection, the following steps have to be performed. First of all group similar posts. But simply grouping similar posts would does not work. Because miscreants slightly modify the content of the posts or use different URLs (e.g., by leveraging URL shortening services) to avoid being detected or blacklisted. To detect market victims, select all posts from user's wall and extracts URLs. Then manually check whether these URL points to an Online Market website. Discard those URLs which does not points to Online Friend Market. Also discard those groups that do not contain any URL in their posts. Note that automatic identification of Account Market websites is probably feasible. However, such techniques are outside the scope of this research.

B. Detecting Market Customers

After the Identification of Victim accounts, next step is to detect market customers. Customer's account is not used for advertisement purpose by the account market team. Thus Customer accounts cannot be identified by detecting posted URL's and grouping them. But it is possible to detect customer account. Unlike other newly created accounts, market customers have large number of friends (ie., the ones purchased from the market). There for consider an account A as being customer who bought friends through online markets if:

- A is befriended by at least tv other accounts that previously identified as victims of Online Friend Markets. The rationale behind this threshold is that market customers are befriended by many free subscribers (i.e., victims) of the market.
- A befriends less than tf other accounts. This threshold discards accounts that periodically befriend a set of users, wait for a number of them to befriend back, and unfriend them. This is a common behavior for accounts looking for friends, but is not indicative on its own of being a Market customer.
- The influence of A on OSN is below the threshold ti. Influence can be defined as a measure that indicates how engaged an account is on OSN. This includes the number of friends the account has, but also the number of posts, and the number of mentions. This threshold allows us to discard those accounts that belong to celebrities. Typically, such accounts have a very unbalanced friends. However, they also have high influence scores, because

people interact with them a lot and share their content with their friends.

- The wall of A does not contain any post indicative ofA being a free subscriber (i.e., victim) to the market.

By setting the thresholds tv, tf, and ti accordingly, it can make sure to detect those accounts that have an anomalous number of friends, compared to other accounts with similar influence.

V. TRUSTFRIENDS: IMPLEMENTATION

In the proposed system, First of all some users should register in Online Social Network namedTrustFriends. Then they can send, receive, accept and reject requests. Real users will send request to their friends or acquaintance. But some peoples create fake identities, ie., a single user pretend to be multiple. This single user sends requests to all its fake profiles and to other users. While receiving a request from an unknown person, by default the chance of accepting that request by a real is very rare. Some users need large number of friends, which is why they will buy friends from online markets. Some users buy friends free, while others buy through payment. TrustFriend account of free users of online markets is used by market team to advertise their website. They will periodically sends URL points to their site through free service activators profile. This is actually the input to the proposed System.

TrustFriends admin is responsible for finding out Sybils and compromised users. To do so, page rank calculation will be performed, it ranks all the users according to the positive and negative votes obtained. For each request send and accept a positive vote will get. For each rejection a negative vote will get. From the ranking, select those users having high page rank and high positive votes as trusted seed. Then propagate vote and aggregate votes. After this step some Sybils will be displayed. Then admin can block these Sybils. To find out other colluding Sybils, select those Sybils obtained from the previous step with higher negative votes as bad seed. Then propagate bad score and detect Sybil. After this step almost all Sybils will be detected. Admin can block them.

Some users compromised their account by purchasing friends from online markets. Compromised users may be victims or customers. To detect Victim accounts, get all posts from all accounts and extract URL from it. Then check each URL manually to check whether it points to a market website or not. An account which post a URL points to market website will be victims. Admin can mark them as victim. Next step is to detect Customers. Those accounts consist of victim detected earlier as friends more than a threshold will be Customers.

VI. RESULT ANALYSIS

To analyze proposed method over existing first I chooses total number of users in TrustFriends OSN as eight, five of them are real and three are Sybils. The number of attack link from Sybil region to Real region is set as three. Then checked how many Sybils will be detected by VoteTrust, existing method and TrustFriends, Proposed method and calculated corresponding Sybil Recall and it is shown in the fig: 7. Suppose that 'O' represents the set of true Sybils existing in the network, and 'I' represents the set of Sybils identified by a defense scheme.

$$\text{Sybil Recall} = | I \cap O | / | O |$$

After that number of users is added to the OSN and varies number attack links from Sybil to real region and evaluated both existing and proposed techniques. In all cases the number of Sybils detected by existing method is lesser than proposed technique. This is because Sybilsdetected by proposed method not only includes Sybils, but also Victims and customers.ie,.Market users

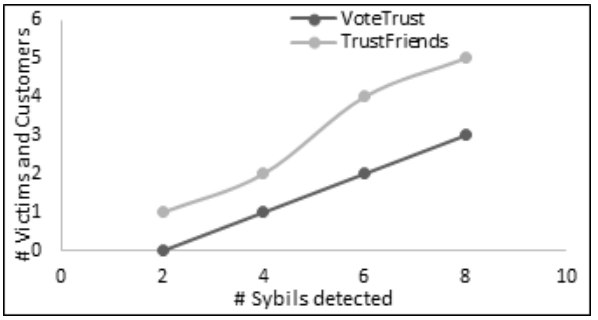

Fig. 7: Sybil Recall Vs Number of attack links for VoteTrust and TrustFriends

Sybils may buy friends from miscreants. Thus detected Sybils may include Victims and Customers. Fig.8 shows number of victims and customers from detected Sybils of both existing and proposed system. From the Fig. 8 it is very clear that the detected Victims and Customers of existing system is less than proposed system. Existing scheme does not have a component to detect market users. But proposed scheme have additional component to detect victims and customers. Fig.8 shows VoteTrust also detects Victims and Customers, these are Sybils who buy friends from miscreants. Victims and Customers detected by TrustFriends not only includes Sybils who buy friends from miscreants, but also includes real users who buy friends from miscreants.

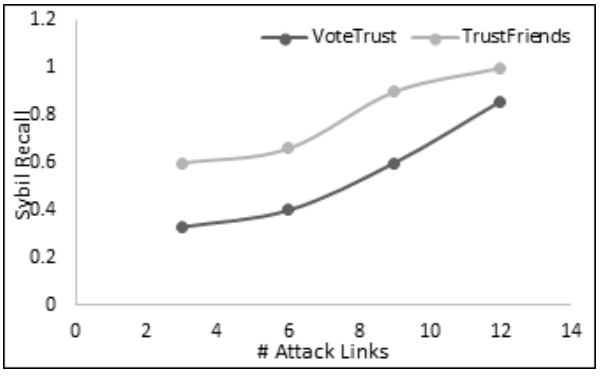

Fig: 8: Number of Victims and Customer Vs Number of detected Sybils

VII. CONCLUSION

This paper presents TrustFriends, a system that detects both Sybils and Compromised accounts. To detect Sybils,VoteTrust algorithm is used. It is a system that leverages user interactions to defend against Sybil attacks. Also used some standard techniques like PageRank-style algorithm to propagate scores, and a technique including global vote aggregation and local community expansion, to exploit the negative links. Thus in the proposed work VoteTrust is considered as a first level defense and combined with a technique which detects compromised users.

To detect compromised users, URLs are extracted from user's wall. Then analyses the extracted URLs to find out whether it belongs to a kind of online markets which provides friends. Users who posts many URLs in their wall points to one or more online markets will be detected as Victims. Those users who befriended many victims will be detected as customers. It is not possible to detect customer through URL extraction, because miscreants, uses only victim accounts to periodically send advertisement posts.

REFERENCES

1. J. R. Douceur, "The Sybil attack," in *Proc. of IPTPS*, March 2002.
2. H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: defending against sybil attacks via social networks," in Proc. Of SIGCOMM, 2006.

3. H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "Sybillimit: A near-optimal social network defense against sybil attacks," in Proc. of IEEE S&P, 2008.

4. W.Wei, F. Xu, C. C. Tan, and Q. Li, "Sybildefender: Defend against sybil attacks in large social networks," in *Proc. of INFOCOM*, 2012.

5. G. Danezis and P. Mittal, "Sybilinfer: Detecting sybil nodes using social networks," in Proc of NDSS, 2009.

6. N. Tran, B. Min, J. Li, and L. Subramanian, "Sybil-resilient online content voting," in Proc. of NSDI, 2009.

7. Frank Li, Prateek Mittal, Matthew Caesar, Nikita Borisov, "SybilControl: Practical Sybil Defense with Computational Puzzles"

8. Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, "Aiding the detection of fake accounts in large scale social online services," in *nsdi*, 2012.

9. Z. Gyongyi, H. Garcia-molina, and J. Pedersen, "Combating web spam with trustrank," in *VLDB*. Morgan Kaufmann, 2004, pp. 576–587.

10. S. Ghosh, B. Viswanath, and F. K. et al, "Understanding and combating link farming in the twitter social network," in *Proc. of WWW*, 2012.

11. VoteTrust: Leveraging Friend Invitation Graph to Defend against Social Network Sybils

12. G. Stringhini, G. Wang, M. Egele, C. Kruegel, G. Vigna, H. Zheng, and B. Zhao, "Follow the green: Growth and dynamics in twitter follower markets," in *ACM Internet Measurement Conference (IMC)*, 2013.

13. Viswanath, A. Post, K. P. Gummadi, and A. Mislove, "An analysis of social network-based sybil defenses," in Proc. of SIGCOMM, 2010.