International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 22 Issue 1 – MAY 2016.

DEFENDING AGAINST SYBIL ATTACK IN SOCIAL NETWORKS

K ARUN (Student) ,V.JAYAPRAKASH, (Student) and R BALAJI SARAN, (Student)
SRM University,Ramapuram,Chennai-600089.

***Abstract*—Open-access distributed systems such as peer-to-peer systems are partic- ularly vulnerable to Sybil attacks, where a malicious user creates multiple fake identities (called Sybil nodes). Without a trusted central authority that can tie identities to real human beings, defending against Sybil attacks is quite challeng- ing.The attacks occur during interactions between the trading peers as a transaction takes place. In this paper, we propose how to address Sybil attack, an active attack, in which peers can have bogus and multiple identities to fake their owns.Peer- to-Peer (P2P) systems take place at the edge of the Internet. Peer communities are established dynamically with peers unknown to each other.In our approach, duplicated Sybil attack peers can be identified as the neighbour peers become acquainted and hence more trusted to each other. A peer can belong to more than one up to n groups. Sybil attacks can been minimized by having common neighbours. Among the small number of decentralized approaches, our recent Sybil- Guard protocol leverages a key insight on social networks to bound the number of Sybil nodes accepted. Despite its promising direction, Sybil- Guard can allow a large number of Sybil nodes to be accepted. Furthermore, SybilGuard assumes that social networks are fast-mixing, which has never been confirmed in the real world.**

I. INTRODUCTION

The concept of social networks, first investigated by sociologists in the1960s, is now one of the key ways social computing is taking place. Social networking sites allow users to create personal profiles, share images and to connect with a large network of friends and often with a lot of strangers. Because of the wide variety of features such as games, puzzles, real time applications, image sharing, instant messaging, and so on, the personal information shared amongst a group can be compromised and this activity also leads to a loss of productivity.There are additionally attacks on the reputation framework associated with social networks with an eye on influencing the integrity of the data or the communication processes of the network . The need for connections is partly driven by the uncertainty that underlies information structures within society. The network networked society must therefore find new ways to connect, which also leads it open to a variety of attacks. It also opens questions related to identity and anonymity. Some of these questions have been traditionally addressed by assigning random sequences to different individuals , as well as the use of cryptography based on quantum mechanics.The main reason for threats in social networking is due to its open architecture and its susceptibility to different viruses . Due to this open structure, the usual culprits such as spam, cross scripting, social engineering can cause much damage. Thus an adversary may masquerade as an honest user and divert the honest user to other pages to spread the malware which leads to a phishing attack or a malicious user may create multiple bogus identities to gain sensitive information from users .

This latter attack where an adversary creates multiple bogus identities to gain sensitive information like full name, SSN, bank details from users to do variety of cyber crimes is the Sybil attack . Sybil attacks are considered to be very crucial in distributed decentralized systems like social networks because a lot of personal information is shared openly and it is impossible to erase the information once uploaded.In P2P networks, which go back to Napster, each task or problem is accomplished by subdividing the task among multiple nodes or peers. Unlike the client server-model, in which the central server provides the resources to the client requests (services provided by web servers and browsers act as clients), all the nodes in a P2P network act as sources and receivers . The peers have their own share of resources such as bandwidth, power, download speed, routing channels to transfer data, computational resources etc. Each peer can communicate and also provide its resources to an external system without the need for central authority.

A P2P network is built on the assumption that each entity in the net- work holds a single identity. When an adversary introduces many bogus identities with a single entity or with no entity at all, a Sybil attack occurs. Using Sybil identities, an adversary may provide false opinions for his/her evil benefits, limit the amount of resources reaching each node, break the trust mechanism in a P2P network and may even cause a Denial- of-Service attack (DoS).

In the initial researches to deal with Sybil attacks, network architectures were re-designed and secure mechanisms such as digital signatures and digital analyzers were used to mitigate the Sybil attacks. Much effort has gone into the study of trust relationships in social networks and community based schemes to reduce the influences of Sybil attacks. This paper reviews Sybil detection schemes based on behavior attributes of Sybil users. It also discusses classification of Sybil attacks, examples of Sybil attacks, social network based Sybil defenses, behavior based Sybil defenses followed by conclusion references.

Classification of Sybil attacks

(i) Direct vs. In-Direct communication

To launch a Sybil attack in a distributed network, the attacker must consider the type of communication between honest nodes and Sybil nodes. If the communication between honest node and Sybil node is direct, i.e. if the attacker can directly communicate with the honest node using fake identities, it is a case of direct communication. However, if the attacker has to use his legitimate identity to communicate with the honest node, and then divert the Sybil data to the

honest node via the legitimate node, it is the case of indirect communication. It is easier for the attackers to launch Sybil attacks in case of direct communication and it is also more difficult to detect such attacks.

(ii) Busy vs. Idle

In a P2P network, normally, only few Sybil identities participate in the network while the others remain idle. The power of the Sybil at- tacker comes from the number of identities he or she holds. If an attacker could afford to get fake identities easily, he or she can make the identities appear more realistic by making them leave and join the network multiple times pretending as an honest node. However, if the number of the Sybil identities are limited, the Sybil identities must participate simultaneously to launch an attack.

(iii) Simultaneous vs. Non Simultaneous

An adversary can create all Sybil nodes simultaneously or introduce them one by one. If the attacker introduces one node at a time and manages to establish different properties for different Sybil nodes, the chances of detecting the Sybil nodes in a P2P network becomes very difficult. However, the attacking time and complexity increases when nodes are introduced at different instances. A simultaneous attack can be per- formed by involving all the Sybil identities simultaneously or a single physical node can change its identities in regular time slots to appear like all the identities are involved simultaneously. In non-simultaneous at- tack, an attacker may bring all his identities into the network slowly over a period of time involving only few identities each time. This can be done by pretending that one identity is leaving the network while the other identity is joining the network. As honest identities generally tend to leave and join the network number of times, the malicious node won t be suspected if they pretend to leave or join the network now and then using different identities. The attacker can also use a number of physical devices to get different identities and can then switch among these identities to perform the attack.

(iv) Insider vs. Outsider

The impact of the Sybil attack depends on whether the attacker is in- side or outside the distributed network. If the adversary is part of the network and holds at least one real identity, then the attacker is called an Insider, otherwise he or she is an outsider. An insider may introduce many fake identities, and pretend to communicate with other nodes using his fake identities. However, for an outsider, it is difficult to introduce Sybil identities into the network, as the distributed network system generally employs some kind of authentication procedure such as passwords, secret codes or encryption processes to access the system. An insider can transmit the false information over the network cloud or receive in- formation from other nodes as the network generally trusts all its internal nodes. However, a Sybil node can easily be detected by monitoring the claimed communication between the suspect node and other nodes.

II. RELATED WORK

A. Sybil Attack problem statement

A Near-Optimal Social Network Defence against Sybil Attacks De- centralized distributed systems such as peer-to-peer systems are particularly vulnerable to Sybil attacks, whereas malicious user pretends to have multiple identities (called sybil nodes). Without a trusted central authority, defending against Sybil attacks is quite challenging. Among the small number of decentralized approaches, our recent Sybil Guard protocol leverages a key insight on social networks to bound the number of sybil nodes accepted. Although its direction is promising, Sybil Guard can allow a large number of sybil nodes to be accepted. Further- more, Sybil Guard assumes that social networks are fast mixing, which has never been confirmed in the real world. This paper presents the novel Sybil Limit protocol that leverages the same insight as Sybil Guard but offers dramatically improved and near-optimal guarantees. The number of Sybil nodes accepted is reduced by a factor of (n), or around 200 times in our experiments for a million-node system. We further prove that SybilLimit guarantee is at most a log n factor away from optimal, when considering approaches based on fast-mixing social networks. Finally, based on three large-scale real-world social networks, we provide the first evidence that real-world social networks are indeed fast mixing. This validates the fundamental assumption behind SybilLimit and Sybil Guards approach.But The SybilLimit along with the SybilGuard guard still faces many inefficiency.

By taking these problem into account in this paper we proposed the system where the SybilGuard protocol uses the SybilInfer algorithm where the Bayes theorem plays an key role in the identification of honest and dishonest node.

III. OVERVIEW

The SybilInfer algorithm takes as an input a social graph G and a single known good node that is part of this graph. The following conceptual steps are then applied to return the probability each node is honest or controlled by a Sybil attacker:

1) A set of traces T are generated and stored by performing special random walks over the social graph G. These are the only information retained about the graph for the rest of the SybilInfer algorithm, and their generation.
2) A probabilistic model is then defined that describes the likelihood a trace T was generated by a specific honest set of nodes within G, called X . This model is based on our assumptions that social networks are fast mixing, while the transitions to dishonest regions are slow. Given the probabilistic model, the traces T and the set of honest nodes we are able to calculate Pr[T —X is honest].
3) Once the probabilistic model is defined, we use Bayes theorem to calculate for any set of nodes X and the generated trace T , the probability that X consists of honest nodes. Mathematically this quality is defined as Pr[X is honest—T]. The use of Bayes theorem.
4) 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 sets X , to only get a few X0 , . . . , XN Pr[X is honest—T]. Using those representative sample sets of honest nodes, we can calculate the probability any node in the system is

honest or dishonest. Sampling and the approximation of the sought marginal probabilities.

IV. Model and Algorithm

Let us denote the social network topology as a graph G comprising vertices V , representing people and edges E, representing trust relationships between people. We consider the friendship relationship to be an undirected edge in the graph G. Such an edge indicates that two nodes trust each other to not be part of a Sybil attack. Furthermore, we denote the friendship relationship between an attacker node and an honest node as an attack edge and the honest node connected to an attacker node as a naive node or misguided node. Different types of nodes. These relationships must be understood by users as having security implications, to restrict the promiscuous behaviour often observed in current social networks, where users often flag strangers as their friends [23]. We build our Sybil defence around the following as- sumptions:

1) At least one honest node in the network is known. In practise, each node trying to detect Sybil nodes can use itself as the apriori honest node. This assumption is necessary to break symmetry: otherwise an attacker could simply mirror the honest social structure, and any detector would not be able to distinguish which of the two regions is the honest one.
2) Social networks are fast mixing: this means that a random walk on the social graph converges quickly to a node following the stationary distribution of the nodes.
3) A node knows the complete social network topology (G) : social network topologies are relatively static, and it is feasible to obtain a global snapshot of the network. Friendship relationships are already public data for popular social networks. This assumption can be relaxed to using sub-graphs, making SybilInfer applicable to decentralised settings.

Here the SybilGuard is taken as the protocol where the Sybil-Infer algorithm is used to detect the honest and the dishonest nodes. The SybilInfer algorithm uses the Bayes Theorem for identifying the honest and the dishonest node from the graph G.

V. Determination of honest Node

In this paper, we propose a framework based on Bayesian inference to detect approximate cuts between honest and Sybil node regions in a social graph and use those to infer the labels of each node. A key strength of our approach is that it, not only associates labels to each node, but also finds the correct probability of error that could be used by peer-to-peer or distributed applications to select nodes.

The first step of SybilInfer is the generation of a set of random walks on the social graph G. These walks are generated by performing a number s of random walks, starting from each node in the graph (i.e. a total of s —V — walks.) A special probability transition matrix is used, defined as follow

$$P_{ij} = \{(\min(1/d_i; 1/d_j)\} \text{ if } i \to j \qquad (1)$$

where di denotes the degree of vertex i in G.

This choice of transition probabilities ensures that the stationary distribution of the random walk is uniform over all vertices jV j. The length of the random walks is

$$l = O(\log|V|) \qquad (2)$$

which is rather short, while the number of random walks per node (denoted by s) is a tunable parameter of the model. Only the starting vertex and the ending vertex of each random walk are used by the algorithm, and we denote this set of vertex-pairs, also called the traces, by T. Now consider any cut X.V of nodes in the graph, such that the a-prior honest node is an element of X. We are interested in the probability that the vertices in set X are all honest nodes, given our set of traces T, i.e.

$$P(X = Honest|T) \qquad (3)$$

. Through the application of Bayes theorem we have an expression of this probability:

$$P(X = Honest|T) = \frac{P(T|X = Honest)P(X = Honest)}{Z} \qquad (4)$$

where Z is the normalization constant given by:

$$Z = \sum_{V} \frac{P(T|X = Honest)}{P(X = Honest)} \qquad (5)$$

Note that Z is difficult to compute because it involves the summation of an exponential number of terms in the size of jV j. Only being able to compute this probability up to a multiplicative constant Z is not an impediment. The a-prior distribution P(X = Honest) can be used to encode any further knowledge about the honest nodes, or can simply be set to be uniform over all possible cuts.

Approximating ProbXX through the traces T provides us with a simple expression for the sought probability, based simply on the number of walks starting in one region and ending in another

$$P(T|X = Honest) = \frac{N_{xx}}{N_{xx} + N_{\bar{x}x}} \cdot \frac{1}{|X|} \qquad (6)$$

This expression concludes the definition of our probabilistic model, and contains only quantities that can be extracted from either the known set of nodes X, or the set of traces T that is assigned a probability. Note that we do not assume any prior knowledge of the size of the honest set, and it is simply a variable jXj or j—X j of the model. Next, we shall describe how to sample from the distribution P(X = HonestjT) using the Metropolis Hastings algorithm.

VI. Preliminary result

Under the SybilGuard Protocol the Infer algorithm using Bayes theorem easily identify the honest nodes.The identified nodes are then kept traces in the graph which make the work efficient.Ones the users request for the network access the nodes are allotted where they can transmit data from source to destination.During this process The Sybil attack detection happens.Using the algorithm it can track the attacks and the attackers.

A. Experimenting in real world

Next we validate the security guarantees provided by Sybil-Infer using a sampled LiveJournal topology. A variant of snowball [9] sampling was used to collect the full data set data, comprising over 100,000 nodes. To perform our experiments we chose a random node and collect all nodes in its three hop neighbourhood. The resulting social network has about 50,000 nodes. We then perform some pre-processing step on the sub-graph:

1) Nodes with degree less than 3 are removed, to filter out nodes that are too new to the social network, or inactive.
2) If there is an edge between A ! B, but no edge between B — A, then A — B is removed (to only keep the symmetric friendship relationships.) We note that despi

te this pre-processing nodes all degreescan be found in the final dataset, since nodes with initial degree over 3 will have some edges removed reducing their degree to less than 3.

After pre-processing, the social sub-graph consists of about 33,000 nodes. First, we ran SybilInfer on this topology without introducing any artificial attack. We found a bottleneck cut diving off about 2; 000 Sybil nodes. It is impossible to establish whether these nodes are false positives (a rate of 6in the LiveJournal network. Since there is no way to establish ground truth, we do not label these nodes as either honest/dishonest.

Next, we consider a fraction f of the nodes to be compromised and compute the optimal attacker strategy, as in our experiments with synthetic data. Figure 5 shows the fraction of malicious identities accepted by SybilInfer as a function of fraction of malicious entitites in the system. The trend is similar to our observations on synthetic scale free topologies. At f = 0:2, the fraction of Sybil identities accepted by SybilInfer is approximately 0:32.

B. Using SybilInfer output optimally

Distributed system applications can, instead of using marginal probabilities of individual nodes, estimate the probability that the particular security guarantees they require hold. High latency anonymous communication systems, for example, require a set of different nodes such that with high probability at least one of them is honest. Path selection is also subject to other constraints (like latency.) In this case the samples returned by SybilInfer can be used to calculate exactly the sought probability, i.e. the probability a single node in the chosen path is honest. Onion routing based system, on the other hand are secure as long as the first and last hop of the relayed communication is honest. As before, the samples returned by

SybilInfer can be used to choose a path that has a high probability to exhibit this characteristic. Other distributed applications, like peer-to-peer storage and retrieval have similar needs, but also tunable parameters that depend on the probability of a node being dishonest. Storage systems like OceanStore, use Rabins information dispersion algorithm to divide files into chunks stored and retrieved to reconstruct a file. The degree of redundancy required crucially depends on the probability nodes are compromised. Such algorithms can use SybilInfer to foil Sybil attacks, and calculate the probability the set of nodes to be used to store particular files contains certain fractions of honest nodes. This probability can in turn inform the choice of parameters to maximise the survivability of the files.

Finally a note of warning should accompany any Sybil prevention scheme: it is not the goal of SybilInfer (or any other such scheme) to ensure that all adversary nodes are filtered out of the network. The job of SybilInfer is to ensure that a certain fraction of existing adversary nodes cannot significantly increase its control of the system by introducing fake Sybil identities. As it is illustrated by the examples on anonymous communications and storage, system specific mechanisms are still crucial to ensure that a minority of adversary entities cannot compromise any security properties. SybilInfer can only ensure that this minority remains a minority and cannot artificially increase its share of the network.

Sybil defence schemes are also bound to contain falsepositives, namely honest nodes labeled as Sybils. For this reason other mechanisms need to be in place to ensure that those users can seek a remedy to the automatic classification they suffered from the system, potentially by making some additional effort. Proofs-of-work, social introduction services, or even payment targeting those users could be a way of ensuring SybilInfer is not turned into an automated social exclusion mechanism.

VII. Deployment strategy

Here the various strategy under the protocol are explained.So far we presented an overview of the SybilInfer algorithm, as well as a theoretical and empirical evaluation of its performance when it comes to detecting Sybil nodes. The core of the algorithm outperforms SybilTrust and SybilLimit, and is applicable in settings beyond which the two systems provide no security guarantees whatsoever. Yet a key difference between the previous systems and SybilInfer is the latters reliance on the full friendship graph to perform the random walks that drive the inference engine. In this section we discuss how this constraint still allows SybilInfer to be used for important classes of applications, as well as how it can be relaxed to accommodate peer-to-peer systems with limited resources code.

VIII. Conclusion

In this paper we presented SybilInfer, an algorithm aimed at detecting Sybil attacks against peer-to-peer networks or open services under the SybilGuard protocol, and label which nodes are honest and which are dishonest. Its applicability and performance in this task is an order of magnitude better than previous systems making similar assumptions, like SybilTrust and SybilLimit, even though it requires nodes to know a substantial part of the social structure within which honest nodes are embedded. SybilInfer illustrates how robust Sybil defences can be bootstrapped from distributed trust judgements, instead of a centralised identity scheme.

SybilInfer is also significant due to the use of machine learning techniques and their careful application to a security problem. Cross disciplinary designs are a challenge, and applying probabilistic techniques to system defence should

not be at the expense of strength of protection, and strategy-proof designs. Our ability to demonstrate that the underlying mechanisms behind SybilInfer is not susceptible to gaming by an adversary arranging its Sybil nodes in a particular topology is, in this aspect, a very import part of the SybilInfer security design.

Yet machine learning techniques that take explicitly into account noise and incomplete information, as the one contained in the social graphs, are key to building security systems that degrade well when theoretical guarantees are not exactly matching a messy reality. As security increasingly becomes a people problem, it is likely that approaches that treat user statements beyond just black and white and make explicit use of probabilistic reasoning and statements as their outputs will become increasingly important in building safe systems.

REFERENCES

[1] ”Optimal Sybil-resilient Node Admission Control”, Nguyen Tran Jinyang Li Lakshminarayanan Subramanian Sherman S.M. Chow, . Courant Institute of Mathematical Sciences New York University.

[2] ”SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks” Haifeng YU, Phillip B. Gibbons and Feng Xiao,February 2008

[3] ”SybilGuard: Defending Against Sybil Attacks via Social Networks” Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, Member, IEEE, and Abraham D. Flaxman

[4] ”SybilDefender: Defend Against Sybil Attacks in Large Social Networks”Wei Wei, Fengyuan Xu, Chiu C. Tan, Qun Li ,The College of William and Mary, Temple University

[5] Yu, H., Gibbons, P. B., Kaminsky, M., and Xiao, F.:SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks. In Proceedings of the 2008 IEEE Symposium on Security and Privacy.

[6] Jain, A. K. and Murty, M. N. and Flynn, P. J. :Data clustering: a review. ACM Comput. Surv, Sept 1999

[7] Chen, Ke. On k-Median clustering in high dimensions. Proceedings of the seven- teenth annual ACM-SIAM symposium on Discrete algorithm, SODA 2006.

[8] Vito Trianni and Thomas Halva Labella and Marco Dorigo. Evolution of Direct Communication for a Swarm-bot Performing Hole Avoidance. ANTS Workshop. 2004.