ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 2, February 2013

Combating Sybil Attacks using SybilGuard

Abhijeet B. Potey[1], Prof.Anjali B.Raut[2]

Department of Computer Science & Engineering, H.V.P.Mandal's College of Engineering & Technology, Amravati, Maharashtra, India.

***Abstract*—This paper presents a Sybil Guard, for combating against Sybil attacks without relying on a trusted central authority. Peer-to-peer and other decentralized, distributed systems are known to be particularly open to Sybil attacks. In aSybil attack, a malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system. Among the small number of decentralized approaches, our recent SybilGuard leverages a key insight on social networks to bind the number of Sybil nodes accepted. Despite its promising direction, SybilGuard can allow a large number of Sybil nodes to be accepted. Furthermore, Sybil Guard assumes that socialnetworks are fast-mixing, which has never been confirmed in the real world. SybilGuard exploits this property to bind the number of identities a malicious user can create. Sybil Guard offers dramatically improved and near optimal guarantees**.

***Index Terms* — Social networks, Sybil attack, SybilGuard, Sybil identity**

I. INTRODUCTION

Sybil attack [3] is the fundamental problem where the attacker can create multiple identities. It is already observed inthe real world peer to peer systems. Social networking is thegrouping of individuals into specific groups, like small ruralcommunities, or a neighborhood sub division .Although social networking is possible in person, especially inthe workplace, universities, and high schools, it is most popularonline. Social networking websites function like an online community ofinternet users.

The local entity has no direct physical knowledge [3] of remote entities; it recognizes that only informational abstractions called identities. The system must ensure that distinct identities refer to distinct entities; otherwise, when thelocal entity selects a subset of identities to redundantly performa remote operation, it can be duped into selecting a singleremote entity multiple times; thereby defeating the redundancy. The illegitimately presents of multiple identities will create aSybil attack [3] on the system. Peer-to-peer and otherdecentralized, distributed systems are known to be particularlyopen to Sybil attacks. In a Sybil attack, a malicious user obtains multiple forged identities [6] and pretends to be multiple, distinct nodes in the system. Without a trusted central authoritythat can tie identities to real human beings, defending againstSybil attacks is quite challenging. When a malicious user'sSybil nodes comprise a large fraction of the nodes in the system, that one user is able to "outvote" the honest users in awide variety of collaborative tasks. The exact form of suchcollaboration and the exact fraction of Sybil nodes thesecollaborative tasks can tolerate may differ from case to case. The ultimate form is reached with a Sybil attack [3], where the attacker creates a potentially unlimited number of fake identities [6] (i.e. Sybil identities) to vote. A generic requirement for upsetting such attacks is that the number of Sybil nodes needs to be properly bounded. Sybil Guard protocol is the solution for defending against Sybil attackswithout relying on a trusted central authority.

***Abhijeet B. Potey** is working as an Assistant Professor and is currently pursuing masters degree program in Computer Science and Engineering in HVPM's College Of Engineering & Technology, Amravati, India , Mobile:+919890161891*

***Anjali B.Raut**is working as Associate Professor and is Head Of Computer Science & Engineering Department of HVPM's College Of Engineering & Technology,Amravati,India, Mobile:+918806172200*

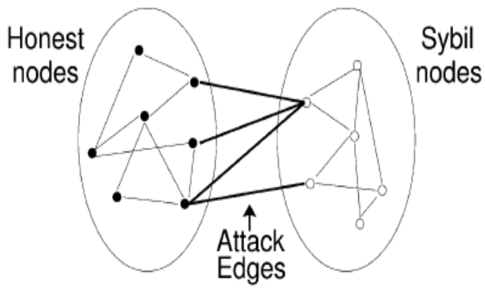

Figure 1**:** the social network with honest nodes and sybil nodes.

A. The Sybil Guard Approach

Sybil Guard is a protocol for defending against Sybil attacks without relying on a trustedcentral authority. In a social network (Fig-1.), the vertices (nodes) are identities in the distributed system and the (undirected) edges correspond to human-established trustrelations in the real world. The edges connecting the honestregion (i.e., the region containing all the honest nodes) and theSybil region (i.e., the region containing all the Sybil identitiescreated by malicious users) are calledattack edges. SybilGuard ensures that the number of attack edges is independentof the number of Sybil identities and is limited by the numberof trust relation pairs between malicious users and honest users.

Sybil Guard is a completely decentralized protocol and enables any honest node V called the verifier to decidewhether or not to accept another node S called the suspect. "Accepting" means that V is willing to do collaborative tasks with S. Sybil-Guard's provable (probabilistic) guarantees hold for verifiers out ofthe (1-ε)n honest nodes, where εis some small constant close to 0.

II. RELATED WORK

A. Sybil Attack In Sensor Networks

Security is important for many sensor network [5] applications. Security in sensor networks is complicated by the broadcast nature of the wireless communication and the lack of tamper-resistant hardware. Sensor nodes have limited storage and computational resources, rendering public keycryptography impractical. The Sybil attack is a harmful attack in sensor networks. In the Sybil attack, a malicious nodebehaves as if it were a larger number of nodes, for example byimpersonating other nodes or simply by claiming falseidentities. An attacker may generate an arbitrary number of additional node identities, using only one physical device.Several novel methods proposed by which a node can verifywhether other identities are Sybil identities, including radioresource testing, key validation for random key predistribution, position verification and registration.

Direct validation is a node directly tests whether another node identity is valid. The most promising method among themethodology is the random key pre-distribution whichassociates a node's keys with its identity. Random key predistribution will be used in many scenarios for securecommunication, and because it relies on well understoodcryptographic principles it is easier to analyze than othermethods. These methods are robust to compromised nodes. Inindirect validation, nodes that have already been verified are allowed to vouch for or refute other nodes. This paper [5] leaves secure methods of indirect validation as future work.

B. Sybil Attack in Recommendation Systems

Recommendation systems [8] can be attacked in variousways, and theultimate attackform is reached with a Sybilattack, where the attacker creates a potentially unlimitednumber of Sybil identities to vote. Defending against Sybilattacks is often quite challenging, and the nature of recommendation systems makes it even harder. Exploiting heavy-tail distribution of typical voting behavior of the honest identities, Carefully identifying whether the system is already getting “enough help” from the (weighted) voters already taken into account or whether more “help” is needed; DSybil[8] can defend against an unlimited number of Sybil identities over time. DSybil provides a growing defense. If the user has usedDSybil for some time when the attack starts, the loss will be significantly smaller than the loss under the worst-caseattack. DSybil into real-world recommendation systems and study the system’s robustness against DDoS.

C. Sybil Attack in Peer to Peer Systems

Networked applications [4] often assume or require thatidentities over network have a one-to-one relationship withindividual entities in the external world. A single individualwho controls many identities can disrupt, manipulate, orcorrupt peer-to-peer applications and other applications thatrely on redundancy; this is commonly called the Sybil attack. Detection of Sybil attack is the problem. To solve thisproblem, a trust game is introduces that makes false claimsfinancially risky for the claimant. The informant [4] willaccept the game if and only if he/she is Sybil with a lowopportunity cost, and the target will cooperate if and only if he/she is identical to the informant. Sybil Game is a moresophisticated game that includes the economic benefit to thedetective oflearning of Sybil and the economic cost toinformant and target of revealing that Sybil’s are present. This paper [4] proves the optimal strategies for each participant. The detective will offer the game if and only if it will determine her choice about using the application in which these identities participate. As future work, intends to develop a protocol to detect Sybil attack.

The methodology applied in [1] are Inferring honest sets, Approximating EXX, representing the ‘gap’ between the case when the full graph is fast mixing, Sampling honest configurations, Experimental evaluation using synthetic data, and the final Experimental evaluation using real world data. Through analytical results as well as experiments on simulated and real-world network topologies that, given standard constraints on the adversary, Sybil Infer [1] is secure, in that it successfully distinguishes between honest and dishonest nodes and is not susceptible to manipulation by the adversary. Results show that Sybil Infer outperforms state of the art algorithms, both in being more widely applicable, as well as providing vastly more accurate results. Modifying the simple minded protocol into a fully-fledged one-hop distributed hash table is an interesting challenge for future work. Sybil Infer can also be applied to specific on-line communities. In such cases a set of nodes belonging to a certain community of interest can be extracted to form a sub-graph. Sybil Infer canthen be applied on this partial view of the graph, to detectnodes that are less well integrated than others into detectnodes that are less well integrated than others in the group.

On-line Voting System [7] is a web based system thatfacilitates the running of elections and surveys online. Thissystem has been developed to simplify the process of organizing elections and make it convenient for voters to vote remotely from their home computers while taking into consideration security, anonymity and providing auditioning capabilities. Online voting system is liable to the Sybil attack where adversaries can out-vote real users by creating several Sybil identities. A basic problem with any user-based content rating system is the Sybil attack where the attacker can out-vote real users by creating many Sybil identities.

SumUp [7], a Sybil resilient online content rating system that advantages a trust networks among users to defend against Sybil attacks with strong security guarantees. SumUp, a Sybil-resilient online content rating system that prevents adversaries from arbitrarily distorting voting results SumUp addresses the basic vote aggregation problem of how to aggregate votes from different users in a trust network in the face of Sybilidentities casting an arbitrarily large number of false votes. By using the technique of adaptive vote flow aggregation, SumUpcan significantly limit the number of false votes cast by adversaries to no more than the number of attack edges in thetrust network SumUp powers the user voting history to further restrict the voting power of adversaries who continuously misbehave to below the attack edges. Aggregate all votes from honest users. Limit the number of false votes from the attacker. Eventually ignore votes from nodes that repetitively cast false votes. Capacity assignment is to construct a vote envelope around the source. SumUp bounds the power of attackers according to the number of attack edges regardless of the number of Sybil identities. SumUp limits the number of false votes to be no more than the number of attack edges with high probability.SumUp can significantly limit the number of bogus votes without affecting the number of honest votes that can be gathered. Additionally, SumUp uses user feedback on false votes to further reduce the attack capacity to below the number of attack edges. The specific feedback mechanism used by SumUp. Capacity assignment should minimize the attack capacity. SumUp collects votes from a trusted source by computing a set of max-flow paths on the trust graph from the source to all voters. The basic design has two limitations. First, although the expected attack capacity is bounded by the number of attack edges, there might be cases where is high when some adversarial identities happen to be close to the source. Second, the basic design only bounds the number of false votes collected on a single object. As a result, adversaries can still cast up to false votes on every object in the system. The real-world benefits of SumUp by evaluating it on thevoting trace of Digg. SumUp has detected many suspicious articles marked as “popular” by Digg. Digg is a social news website. Digg is a place for people to discover and sharecontent from anywhere on the web.

III. SYSTEM MODEL AND ATTACK MODEL

The system has honest human beings as honest users, each with one honest identity/node. Honest nodes obey the protocol. The system also has one or moremalicious human beings as malicious users, each with one ormore identities/ nodes. To unify terminology, we call allidentities created by malicious users as Sybil identities/nodes. Sybil nodes are Byzantine and may behave arbitrarily. AllSybil nodes are colluding and are controlled by an adversary. A Compromised honest node is completely controlled by theadversary and hence is considered as a Sybil node and not asan honest node.

Every node is simultaneously a suspect and a verifier. We assume that each suspect S has a locally generated public/private key pair, which serves to prevent the adversary from “stealing” S’s identity after S is accepted. When a verifier V accepts a suspect S, V actually accepts S’s public key, which can be used later to authenticate.

IV. SYBIL GUARD PROTOCOL

Sybil guard has two component protocols: asecure randomroute protocol and a verification protocol. The first protocol runs in the background and maintains information used by the second protocol.

A. *Random Walk and Random Routes*

Sybil Guard uses a special kind of random walk, called random routes, in the social network. In a random walk, at each hop, the current node flips a coin on the fly to select auniformly random edge to direct the walk (the walk is allowedto turn back). For random routes, each node uses a precomputed random permutation—“x1, x2,…xd,” where d is the degree of the node—as a one-to-one mapping from incoming edges to outgoing edges. A random route entering via edge i will always exit via edge x_i. This pre computed permutation, or routing table, serves to introduce external correlation across multiple random routes. Namely, once two randomroutes traverse the same directed edge, they will merge andstay merged (i.e., they converge). Furthermore, the outgoingedge uniquely determines the incoming edge as well; thus therandom routes can be back-traced. These two properties are key to Sybil Guard’s guarantees. As a side effect, such routingtables also introduce internal correlation within a singlerandom route. Namely, if a random route visits the same nodemore than once, the exiting edges will be correlated. In SybilGuard, a random walks starting from an honest node in the social network is called escaping if it ever crosses any attack edge.

B. *Secure Random Route Protocol.*

We first focus on all the suspects in SybilGuard i.e., nodes seeking to be accepted. Figure 2, Presents thepseudo-code for performing random routes. In the protocol, each node has a public/private key pair and communicates only with its neighbors in the social network.Every pair of neighbors shares a unique symmetric secret key (the edge key, established out of band for authenticating eachother. A Sybil node M1 may disclose its edge key with somehonest node A to another Sybil node M2. However, because allneighbors are authenticated via the edge key, when M2 sends a message to A,A will still route the message as if it comesfrom M1.In the protocol, every node has a pre computed random permutation x1 x2,…xd(d being the node’s degree) asits routing table. The routing table never changes unless thenode adds new neighbors or deletes old neighbors. A suspect S starts a random route along a uniformly random edge (of S) and propagates alongthe routeitspublickey Kstogetherwith acounterinitialized to 1.Every node along the route increments the counter and forwards the message until the counter reaches w, the length of a random route. Sybil Limit’s end guarantees hold even if Sybil nodes (on the route) modify the message. In Sybil Guard, w is chosen to be the mixing time of the honest region of thesocial network. All these random routes need to be performedonly one time (until the social network changes) and the relevant information will be recorded.

Executed by each suspect S:
1. S picks a uniformly random neighbor Y;

2. S sends to Y :(1, S’s public key Ks, MAC (1||Ks,)) with the MAC generated using the Edge Key between S and Y;

Executed by each node B upon receiving a message (i, Ks, MAC) from some neighbor A:

1. Discard the message if the MAC does not verify or i<1or i>w;

2. if (i=w) {record Ks under the edge name “KA→KB ” where KA and KB are A’s and B ’s public key, respectively;} else {

3. look up the routing table and determine to which neighbor (C) the random route should be directed;

4. B sends to C: (i+ 1, Ks, MAC ((i+ 1)|| Ks)) with the MAC generated using the edge key between B and C;
}

Figure 2: Secure random route protocol

C. Verification protocol.

After the secure random route protocol stabilizes, a verifier can invoke the verification protocol in Figure 3 to determine whether to accept a suspect S. The intersection condition requires that S's tails and V's tails must intersect (instance number is ignored when determining intersection), 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 maintains r counters corresponding to its r tails. Every accepted suspect increment the "load" of some tail. The balance condition requires that accepting S should not result in a large "load spike" and cause the load on any tail to exceed hmax(log r, a).Here a, is the current average load across all V 's tails, and h >1 is some universal constant that is not too small. In comparison, Sybil Guard does not have any balance condition. The verification protocol canbemadehighlyefficient. Theadversary mayintentionallyintroduceadditionalintersectionsintheSybilr egionbetween S's and V's escaping tails.

1. Ssends toV its public key Ks andS's set of tails {(j, K_A, KB) |S's tail in thejth s-instance is theedge "A→B" and K_A (K_B) isA's (B's) public key};

2.V computes the set of intersecting tails X={(i, K_A,K_B) | (i, K_A,K_B) isV's tail and (j, K_A,K_B) isS's tail};

3. For every (i,K_A,K_B)Є X ,V authenticatesBusing$K_B$and asksBwhetherSisregisteredunder"K_A→K_B"If not, remove (i,K_A,K_B) fromX ;

4. ifX is empty then rejectSand return;

5. Let$a = (1 + \sum_{i=1}^{r} ci)/r$ and b=h.max (log r, a);

6.Let c_{min}bethe smallest counter among thoseci'scorresponding to(i,K_A,K_B) that still remain inX

7. if (c_{min}+ 1) >b) then rejectS;otherwise, incrementc $_{min}$and acceptS;

Figure 3Verification protocol

D. Estimating the number of routes needed

New SybilGuard uses a novel and perhaps countersintuitivebenchmarking technique [9]to address the number of routesproblem by mixing the real suspects with some randombenchmark nodes [9]that are already known to be mostlyhonest.

Every verifierV maintains two sets of suspects: thebenchmark setKand thetest set T. Thebenchmark set is constructed by repeatedly performing random routes of lengthwand then adding the ending node (called thebenchmark node) toK. LetK $^+$andK$^-$be the set of honest and Sybilsuspects inK, respectively. SybilGuard does not know whichnodes inKbelong toK $^+$.However, a key property here is thatbecause the escaping probability [2] of such random routes is O(1) , even without invoking Sybil Guard, we are assured that|K$^-$|/ |K |=O(1). Thetest set T contains the real suspects thatV wants to verify, which may or may not happen to belong toK. We similarly defineT $^+$and T$^-$. Our technique will hinge uponthe adversary not knowingK $^+$or T$^-$even though it may knowK $^+$UT$^+$andK$^-$U T$^-$.

To estimate r, a verifier V starts from r =1 and then repeatedly doubles r. For everyr value, verifies all suspectsinKandT. It stops doubling when most of the nodes inK areaccepted, and then makes a final determination for eachsuspect inT. The benchmarking technique may appear counterintuitive in two aspects. First, if SybilGuard uses an underestimated r, it will be the adversary that helps it to accept mostof the honest nodes. Second, the benchmark set is itself a setwith fraction of Sybil nodes. That an application can just usethe nodes in directly and avoid the full Sybil Guard protocol

V. CONCLUSION

This paper presented Sybil Guard, a near-optimal defense against Sybil attacks using social networks. Sybil Guard improvement derives from the combination of multiple novel techniques: 1) leveraging multiple independent instances of the random route protocol to perform many short random routes; 2) exploiting intersections on edges instead of nodes;3) using the novel balance condition to deal with escaping tails of the verifier; and 4) using the novel benchmarking techniqueto safely estimate.

As future work, we intend to implement Sybil Guard within the context of some real-worldapplications and demonstrate its utility.

ACKNOWLEDGMENT

My thanks to the Head &Guide, Prof. A.B.Raut and Principal Dr.A.B.Marathe, who provided me constructive and positive feedback during the preparation of this paper.

REFERENCES

[1] G. Danezis and P. Mittal, "SybilInfer: Detecting sybil nodes using social networks," presented at the NDSS, 2009.

[2] M. Mitzenmacher and E. Upfal," Probability and Computing." Cambridge,U.K.: Cambridge Univ. Press, 2005.

[3] J. Douceur, "The Sybil attack," inProc. IPTPS, 2002, pp. 251–260.

[4] N. B. Margolin and B. N. Levine, "Informant: Detecting sybilsusing incentives," inProc. Financial Cryptography, 2007, pp. 192–207.

[5] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis & defenses," in Proc. ACM/IEEE IPSN , 2004, pp.259–268.

[6] Baptiste Pretre, Semester Thesis, "Attacks on Peer to Peer Networks".

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

[8] H. Yu, C. Shi, M. Kaminsky, P. B. Gibbons, and F. Xiao, "DSybil:Optimalsybil-resistance for recommendation systems," inProc. IEEE Symp. Security Privacy, 2009, pp. 283–298.

[9] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "Sybil Limit: A near optimal social network defense against sybil attacks," inProc.IEEE/ACM transactions on networking, Vol. 18, No. 3, June 2010