ISSN No. 0976-5697

Volume 5, No. 1, Jan-Feb 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Survey on Defense Mechanism for Sybil Attacks in Large Social Networks

S.Krishnaveni*, Dr. A.V.Senthil Kumar
Research Scholar, Director, Department of mca
Hindusthan College of Arts &Science,
Coimbatore, india.
sks.krishnaveni@gmail.com*, avsenthilkumar@yahoo.com

Abstract- A social network is a social structure that is made up of nodes which represents the individuals or associations. The Sybil attacks are more vulnerable that affects the Peer-to-Peer and other decentralized systems. The Sybil identities cooperate the system and pollute the system with false information. Sybil identities can restrain the honest identities in a various tasks including online content ranking, distributed hash table routing, file sharing system, reputation systems and Byzantine failure defenses. With Sybil nodes comprising a large fraction of the nodes in the system, the malicious user is capable to "out vote" the honest users, effectively breaking prior defenses against malicious behaviors. Therefore, an effectual defense mechanism against Sybil attacks would remove a primary practical obstruction to collaborative tasks on peer-to-peer (p2p) and other decentralized systems. To defend against Sybil attacks, to monitor each nodes historical behavior is often insufficient because Sybil nodes can behave nicely initially and then launch an attack. To mitigate the Sybil attacks, different decentralized mechanisms are used such as Sybil Infer, Sybil Guard, and Sybil limit to decide whether a suspect node is Sybil. In particular, we analyze the mechanisms how the Sybil attacks can be mitigated.

I. INTRODUCTION

Distributed Systems are susceptible to Sybil attacks in that an adversary generates many bogus identities called Sybil identities and compromises the running of the system with false information. The Sybil identities can restrain the honest identities in a various tasks, including voting schemes for email spam to implicit collaboration in redundant routing and data replication in Distributed Hash Tables. The Sybil attacks can be mitigated by assuming the existence of a trusted authority, in which rate-limit the introduction of fake identities by requiring the users to provide some credentials, like social security number, or by requiring payment. But such requirements will prevent users from accepting these systems, as they enforce further burdens on users.

Peer-to-peer systems normally rely on the existence of multiple, independent remote entities to moderate the threat of hostile peers [1]. Many systems replicate computational or storage tasks among the several remote sites to protect against integrity violations. To exploit the redundancy in the system needs the ability to decide whether two ostensibly different remote entities are essentially different. To reduce the threats many such systems employ redundancy. On the other hand, if a single faulty entity can present multiple identities, it can manage a considerable fraction of the system, thereby undermining this redundancy.

For the Sybil defense mechanisms, there are two schools namely the centralized and decentralized defense schemes [4]. Centralized defenses assume the existence of an authority which is capable of doing admission for the network. The role is to rate limit the introduction of fake identities to make sure that the fraction of corrupt nodes remains under a certain threshold. The practicalities of running such an authority are very system-specific and in general it would have to act as a Public Key Certification Authority as well as a guardian of the moral standing of the nodes introduced a very complex problem in practice. The centralized solutions are also at odds with the decentralization guiding principle of peer-to-peer systems. Decentralized approaches recognize the difficulty in having a single authority vouching for nodes and to allocate this task across all nodes of the system.

In the following survey, various mechanisms are investigated to mitigate the Sybil attacks. In a social network, two user identities share a link if a relationship is established between them. Each identity is denoted as a node in the social graph. To avoid the adversary from creating many Sybil identities, all the earlier Sybil defense schemes are built upon the assumption that the number of links between the Sybil nodes and the honest nodes, which is called as attack edges, is restricted. Although, an adversary can create many Sybil nodes and link them in a random way, there will be a small cut between the honest region and the Sybil region. In this small cut consists of the attack edges and its removal disconnects the Sybil nodes from the rest of the graph, that is leveraged by previous schemes to identify the Sybil nodes. But this method is non-trivial because identifying small cuts in a graph is an NP-hard problem. Sybil guard and Sybil limit are the decentralized mechanisms to determine whether a suspect node is Sybil or not. To discover the Sybil nodes, these schemes leverage random routes, a special kind of random walks in which every node utilizes the pre-computed random permutation as a one-to-one mapping from incoming edges to outgoing edges. Sybil Infer is a centralized defense mechanism, which leverages a Bayesian inference method that assigns a Sybil probability, signifying the degree of certainty, to every node in the network.

II. SYBIL DEFENSE MECHANISMS

A. Sybil Guard Approach:

Haifeng Yu and Michael Kaminsky [2] proposed Sybil Guard a novel decentralized protocol is used for limiting the corruptive influences of Sybil attacks. The range of decentralized distributed system increases, there is increase in the malicious behavior of the nodes. A trusted central authority that issues and verifies credentials unique to an

actual human being can avoid Sybil attacks easily. The central authority may also instead require a payment for each identity. Regrettably, there are many scenarios where such designs are not desirable. A novel decentralized protocol called Sybil Guard that includes Sybil attacks exploiting IP harvesting and even some Sybil attacks launched from both nets outside the system.

This design is based on a unique insight regarding social networks in which identities are nodes in the graph and edges connecting are human-established trust relations. The edges connecting the honest region and the Sybil region are called attack edges. This protocol ensures that the number of attack edges is independent of the number of the number of Sybil identities and it is limited by the number of trust relation pairs between malicious users and honest users. The main insight is that if malicious users create too many Sybil identities, the graph becomes "strange" in the sense that it has a small quotient cut i.e., a small set of edges whose removal disconnects a large number of nodes from the rest of the graph. However social networks do not tend to such cuts. To search such cuts, the global topology and verify each edge with its two Endpoints is needed. Sybil guard relies on the verifiable random walk in the graph and intersections between such walks. These walks are designed so that the small quotient cut between the Sybil region and the honest region can be used against the malicious users, to bound the number of Sybil identities that they can create. But this Sybil guard suffers from high false negatives as each attack edge may introduce Sybil nodes without being detected.

B. Sybil Limit Approach:

Haifeng Yu and Phillip B. Gibbons [3] proposed a novel Sybil limit protocol which leverages the same insight as Sybil guard but offers radically improved and near-optimal guarantees. Decentralized distributed systems are specifically vulnerable to Sybil attacks. Previously the Sybil Guard mechanism is used but there is a problem it suffers from high false negatives, as each attack edge may introduce Sybil nodes being detected. To call it is Sybil Limit because it limits the number of Sybil nodes accepted and it is near-optimal and thus pushes the approach to the limit. Sybil limit utilizes the same technique as Sybil guard to do random routes, the overhead incurred is dissimilar because Sybil limit uses multiple instances of the protocol with a shorter route length. Using instances of the random route protocol does not acquire extra storage or communication overhead by itself. Firstly, a node does not need to store routing tables, while it can keep a single random seed and then create any routing table on the fly as needed. Secondly, messages in different instances can be readily combined to diminish the number of messages. Lastly, the total number of bits a node requires to send in the protocol is linear with the number of random routes times the length of the routes. In this method, every node has a public/private key pair, and communicates only with its neighbors in the social network.

For authenticating each nodes, every pair of neighbors share a unique symmetric secret key. Every node has a pre-computed random permutation as its routing table. The routing table never changes unless the node adds new neighbors or deletes old neighbors. Every node along the route increments the counter and forwards the message until the counter reaches the value, the length of a random route. But the limitation in this method is does not provide high accuracy to detect the Sybil nodes.

C. Sybil Infer Approach:

George Danezis and Prateek Mittal [4] proposed Sybil Infer algorithm to label the nodes in a social network as honest users or Sybil controlled by an adversary. The Peer-to-peer systems allow cooperating users without need of centralized infrastructure. But due to the lack of any centralized control over identities there is vulnerable to Sybil attacks. Sybil Infer lies in a probabilistic model of honest social networks, and an inference engine which returns potential regions of dishonest nodes. The main contribution is to detect Sybil nodes in a social network, which makes use of all information that available to the defenders. The proper model underlying this approach casts the problem of detecting Sybil nodes in the context of Bayesian inference: For a given set of stated relationships between the nodes, the task is to label nodes as honest or dishonest. Based on the simple and generic assumptions, like the fact that social networks are fast mixing. In the social graph, to sample cuts according to the probability divide it into honest and dishonest regions. These samples not only allow us to label nodes as honest or dishonest and also to combine with each label output by the algorithm a degree of certainty. In the Sybil infer method, which takes as an input a social graph and a single known good node that is part of this graph. After that this can be applied to return the probability each node is honest or controlled by a Sybil attacker. A set of traces are generated and stored by performing special random walks over the social graph.

A probabilistic model is then defined that expresses the likelihood a trace was created by a specific honest of nodes within graph. Once the probabilistic model is defined, a Bayes theorem is used to calculate for any set of nodes and the generated trace. Finally, to calculate the probability of any node in the system to identify whether it is honest or dishonest. But in this approach the overall complexity is high.

D. Gatekeeper Decentralized Sybil Defense Scheme:

Nguyen Tran and Jinyang Li proposed [5] Gatekeeper a decentralized Sybil admission protocol that uses an improved version of the ticket distribution algorithm to perform node admission control in a decentralized fashion. In the open systems there is vulnerable to Sybil attacks because there is lack of strong user identity. The attacker can use a huge number of fake identities to pollute the system with bogus information. Gatekeeper executes the ticket distribution algorithm from multiple randomly select vantage points and combines the results to perform decentralized admission control. Usually, open systems rely on the central authority who employs computational puzzles to reduce the Sybil attack. But these solutions can only limit the *rate* with which the attacker can introduce Sybil identities into the system instead of the total number of such identities. Under constraints that attack edges are hard to establish and there is only a constant number of them, Gatekeeper is an optimal decentralized protocol for the Sybil-resilient admission control problem. A node which acts as an admission controller decides which of the other nodes should be admitted into the system.

This process can be either be creating a list of admitted nodes or determining whether a particular suspect node can

be admitted or not. In the centralized setting, one usually assumes the existence of a trusted controller which performs admission control on behalf of all nodes. In the Gatekeeper control consists of two phases. One is bootstrap phase in which each node acts as a ticket source to disseminate tickets throughout the network and another one is admission phase in which a node acts as an admission controller. Every node performs decentralized ticket distribution to reach more than half of the honest nodes. After all ticket sources have bootstrapped, each node can execute its own admission control to determine upon a list of nodes to be admitted into the system. But this scheme suffers from high false positive and negative rates and cannot efficiently discover Sybil nodes on the real-world asymmetric social topologies.

E. Ant farm: Content Distribution System:

Ryan S. Peterson and Emin Gun Sirer [6] proposed an efficient content distribution system called Ant farm, based on managed farms. Content distribution has emerged as a critical application as demand for high fidelity multimedia content has soared. Swarming protocols have been used to restrict technical and legal attacks to avoid central authority. But the highly decentralized nature of unmanaged swarming systems leads to a performance penalty for legitimate content distributors. The objective of Ant farm is to distribute a huge set of files to large set of clients. Managed swarms initiate a hybrid approach to swarming systems in that they allow a coordinator, usually managed by the content distributor to control the behavior of the swarms. Ant farm is designed to increase the system-wide benefit of the critical resource, seeder bandwidth. Every Ant farm peer provides resources to other participants, and receives unforgivable tokens in return and receives credit for its tokens to the central coordinator.

The Ant farm token protocol forces to every participant to disclose its upload contributions to the swarm coordinator that facilitates the coordinator to conclude swarm dynamics and assign bandwidth to opposing swarms. This allows the coordinator to exert control whereas make possible peers to utilize micro-optimizations, like as optimistic unchoking for peer discovery, tit-for-tat for the selection of peer-to-peer systems, and rarest first, to progress the efficiency of swarming downloads. Given the internal dynamics of a set of swarms, to optimize the bandwidth among the swarms such that average download latencies are minimized across all peers. If preferred, the algorithm can assure a minimum service level to definite swarms, avoid starvation, and enforce prioritization among swarms. Minimizing the average download latency in turn enables a content distributor to achieve the best possible service from the available bandwidth. A wire-level protocol is utilized for accurately measuring the internal dynamics of individual swarms by making peer contributions evident to the coordinator, enabling the coordinator to optimally distribute bandwidth among the competing swarms. But this method limits the rate at which Sybil identities are introduced into the systems, but they cannot identify the existing Sybil identities.

F. Security and Privacy in Online Social Networks:

Ed Novak and Qun Li [7] consider the major issues concerning privacy and security in online social networks. In the online social network there is a wealth of information about its users embedded in the social graph. Particularly, there are two categories of information: explicit and implicit information. Explicit information is information which is stated by the user on purpose. Explicit information is not essentially accurate. There is also implicit information. This is information that can be incidental about a user or a community based on explicit information. Much of the information which is usually published by users in an online social network is particularly sensitive. It is because of this sensitive information, both implicit and explicit, that privacy and security concerns are raised. Firstly to discuss that the objective to protect user data from the various attack vantage points containing other users, advertisers, third party application developers and the online social network provider itself. After that, to cover social network inference of user attributes, locating hubs, and link prediction.

Because online social networks are so saturated with sensitive information, network inference plays an important role. Online social networking has stirred an interesting new trend of users sharing their location information with applications. This permits online social networks to present targeted, dynamic content based on location information. On the other hand, this again raises security and privacy issues because location information is, by its nature sensitive and time-sensitive. Mobile online social networks make extensive use of user location. A mobile online social network is a network that users access primarily through mobile devices. All of this brings up interesting security and privacy concerns. But in this method has high computational complexity and NP-hard problem.

G. Automated Identity Theft Attacks:

Leyla Bilge, Thorsten Strufe [8] proposed to investigate how easy it would be for a probable attacker to launch automated crawling and identity theft attacks against a number of popular social networking sites in order to gain access to a large volume of personal user information. Social networking sites have been increasing recent years. Unlike a Sybil attack in which the attacker aims to subvert a reputation system of a peer to peer or a social network by creating a large number of pseudonymous entities. In the first attack we clone an already existing profile in a social network and to send friend requests to the contacts of the victim. Therefore, we are capable to “steal” the contacts of a user by forging his identity and creating a second, identical profile in the same social network. Having access to the contacts of a victim, therefore, means that we can access the sensitive personal information provided by these contacts. In the second attack to present the effectual and feasible to launch an automated, cross-site profile cloning attack. This type of attack is capable to automatically find users who are registered in one social network, but who are not registered in another. We can then clone the identity of a victim in the site where he is registered, and forge it in a social networking site where he is not registered yet. After that effectively generated the forged identity, and then automatically attempt to rebuild the social network of the victim by contacting his friends that we have identified to be registered on both social networking sites.

H. Sybil Defense Schemes to Detect local Communities:

Bimal Viswanath and Ansley Post [9] proposed Sybil defense schemes to detect the local communities around a trusted node. Nodes which have better connectivity to the

trusted node are ranked higher and consider as a trustworthy node. Despite their considerable differences, all Sybil defense schemes rank nodes similarly—nodes within local communities around the trusted node are ranked higher than nodes in the rest of the network. Thus, Sybil defense schemes work by effectively detecting local communities.

The finding has important implications for both existing and future designs of Sybil defense schemes. Firstly, to show that there is an opportunity to leverage the substantial amount of prior work on general community detection algorithms in order to defend against Sybil. Secondly, the analysis reveals that the fundamental limits of current social network-based Sybil defenses: to demonstrate that networks with well-defined community structure are intrinsically more susceptible to Sybil attacks, and that, in such networks, Sybil can cautiously target their links in order make their attacks more effectual. To motivate us to investigate whether a class of algorithms, known as community detection algorithms which attempt to discover such clusters of nodes directly, could be used for Sybil defense. To find that it is possible to use off-the –shelf community detection algorithms to identify Sybil. Secondly, the insight also hints at the restrictions of relying on communities for identifying Sybil. For Sybil defense schemes to perform well, all non-Sybil nodes require to form a single community that is discernible from the group of Sybil nodes. On the other hand, users in many social networks form multiple communities that are interconnected rather meagerly.

I. Sybil Attack Without Using Logically Centralized Authority:

John R. Douceur [10] proposed to detect the Sybil attack without using a logically centralized authority. Because in a distributed computing atmosphere, for originally unknown remote computing elements to present convincingly distinct identities. With no logically central, trusted authority to vouch for a one-to-one correspondence between entity and identity, it is always probable for an unfamiliar entity to present more than one identity, except under conditions that are not practically realizable for large-scale distributed systems. Peer-to-peer systems usually rely on the existence of multiple, independent remote entities to alleviate the threat of hostile peers. It dissimilar identities for remote entities are not recognized either by an explicit or implicit certification, these systems are vulnerable to Sybil attacks. Systems which rely on the implicit certification should be intensely careful of this reliance, however apparently not related changes to the relied-upon mechanism can decide the security of the system. In the non-existence of an identification authority, a local entity ability to distinguish among distinct remote entities that depends on the postulation that an attacker resources are restricted. Entities can thus issue resource-demanding challenges to legalize identities, and entities can cooperatively pool the identities they have individually authenticated.

J. The Built a online Social Network:

Yazan Boshmaf et.al proposed a conventional web-based botnet design and built a Social bot Network. Online Social Networks (OSNs) such as Face book and Twitter have far exceeded the usual networking service of connecting people together [11]. Social bot is nothing but a new breed of computer programs and they can be used to influence online social network users. A social bot is automation software which organizes an account on a particular online social network and it has a capability to perform basic activities such as posting a message and sending a connection request. The social bot is o compromise the social graph of a targeted online social network by infiltrating its users so as to reach an influential location. To compute how susceptible online social networks are to a large-scale infiltration by social bots: computer programs which control online social network accounts and mimic real users.

K. Large – Scale Extent and Analysis of Multiple Online Social Networks:

Alan Mislove et.al proposed a large-scale extent and analysis of the structure of multiple online social networks [12]. The online social network is organized around users. When the user participating in the network, publish their profile and any content after that generate links to any other users with whom they associate. The resulting social network offers a basis for maintaining social relationships, for identifying users with related interests, and for locating content and knowledge that has been donated or endorsed by other users. An in-depth understanding of the graph structure of online social networks is essential to estimate current systems, to propose future online social network based systems, and to understand the impact of online social networks on the Internet. To present a large-scale measurement study and analysis of the structure of four popular online social networks. The data collected from multiple websites facilitates us to discover general structural properties of online social networks. To believe that ours is the first study to scrutinize multiple online social networks at scale. To attain the data by crawling publicly accessible information on these sites, and to make the data obtainable to the research community. Additionally, to validating the power-law, small-world and scale-free properties previously observed in offline social net works, to present insights into online social network structures. To observe a high degree of reciprocity in directed user links, most important to a strong association between user in degree and out degree.

This differs from content graphs like the graph formed by Web hyperlinks, in which the popular pages and the pages with many references are dissimilar. To identify that online social networks contain a large, strongly associated core of high-degree nodes, enclosed by many small clusters of low-degree nodes. This recommends the high-degree nodes in the core are important for the connectivity and the flow of information in these networks.

L. Detection To Spam Filtering And Social Web Search:

Alessandra Sala et.al suggested measurement-calibrated graph models for detecting Sybil attacks. In the online social networking systems, a complex graph datasets is crucial to research. The graph data provide crucial assessment of new systems and applications ranging from community detection to spam filtering and social web search [13]. Because of the high time and resource costs of collecting real graph datasets via direct evaluations researchers are anonymizing and sharing a small number of valuable datasets with the community. On the other hand, performing experiments by utilizing shared real datasets faces has three key disadvantages: concerns that graphs can

be de-anonymized to disclose private information, the large data sets cost is increased, and in which a small number of obtainable social graphs restricts the statistical confidence. Graph models to a real social graph, eliminate a set of model parameters, and utilize them to produce multiple synthetic graphs statistically similar to the original graph. While numerous graph models have been planned, it is uncertain if they can produce synthetic graphs that accurately match the properties of the original graphs. The realistic synthetic graph is generated by the graph models, it also highlights the fact that current graph metrics remain incomplete, and some applications represent graph properties that do not map to existing metrics.

M. Scale Free Networks:

Holger Ebel et.al suggested an attempt is made to combine ideas from the two fields of "small-world networks" and "scale-free networks" in order to tackle the dynamics of social networks and the dynamical appearance of the small-world structure [14]. A remarkable quality of many complex systems is the occurrence of large and stable network structures as, for example, networks on the protein or gene level, ecological webs, communication networks, and social networks. Simple models based on disordered networks are quite successful in describing basic properties of such systems. When addressing topological properties, however, neither random networks nor regular lattices provide an adequate framework. Particularly, a simple dynamical model for the evolution of acquaintance networks is studied. It produces highly clustered networks with small average path lengths that scale logarithmically with network size. Furthermore, for small death-and-birth rates of nodes this model converges towards scale-free degree distributions, in addition to its small-world behaviour. Basic ingredients are a local connection rule based on "transitive linking," and a finite age of nodes.

N. Geographic Regional Networks:

Christo Wilson et.al The information sharing on the internet and in communication the Social networks are admired. The fashionable social networks such as MySpace and Face book presents communication, storage space and community applications for hundreds of millions of users. These social networks provide platforms for organizing events, user to user communication, and are among the Internet's most popular destinations. Unlike other social networking websites in which all users exist in a global search-space, Face book is calculated around the concept of "networks" which organizes users into membership-based groups. Each network can represent an educational institution, a company or organization (called work networks), or a geographic (regional network) location. Face book authenticates membership in college and work networks by verifying that users have a valid e-mail address from the associated educational or corporate domain. Users can authenticate membership in high school networks through confirmation by an existing member. In contrast, no authentication is required for regional networks. A user's network membership decides what information they can access and how their information is accessed by others. By default, a user s profile contains Date of Birth, address; contact information, Mini-Feed, Wall posts, photos, and photo comments are viewable by anyone in a shared network. Users can change privacy settings to limit contact to simply friends, friends-of-friends, lists of friends, no one. Although membership in networks is not necessary, Face book's default privacy settings encourage membership by making it very difficult for non-members to access information inside a network.

III. CONCLUSION

Peer-to-peer and other decentralized, distributed systems are known to be predominantly susceptible to Sybil attacks. In this survey we analyze the Sybil defense mechanisms to mitigate the Sybil attacks. Because in Sybil attacks an adversary creates many false identities called Sybil identities and pollutes the system with fake information. The Sybil mechanisms such as Sybil Guard and Sybil Limit both rely on the assumption that social networks are fast mixing and the number of attack edges is limited. Sybil Infer a centralized Sybil defense algorithm leverages a Bayesian inference approach which assigns a Sybil probability, indicating the degree of certainty, to each node in the network. Gatekeeper is another decentralized Sybil defense scheme which heavily relies on the assumption that the social networks are random expander. But these mechanisms are not effective for detect the Sybil attacks. At the end of this survey, conclude that the effective mechanism is introduced to identify the Sybil nodes.

IV. REFERENCES

[1]. J.R. Douceur, "The Sybil Attack," Proc. Revised Papers First Int'l Workshop Peer-to-Peer Systems (IPTPS '01), 2002.

[2]. H. Yu, M. Kaminsky, P.B. Gibbons, and A. Flaxman, "SybilGuard: Defending against Sybil Attacks via Social Networks," Proc. ACM SIGCOMM, 2006.

[3]. H. Yu, P.B. Gibbons, M. Kaminsky, and F. Xiao, "Sybil Limit: A Near-Optimal Social Network Defense against Sybil Attacks," Proc. IEEE Symp. Security and Privacy, 2008.

[4]. G. Danezis and P. Mit, "Sybil infer: Detecting Sybil Nodes Using Social Networks," Proc. Network and Distributed System Security Symp. (NDSS), 2009.

[5]. N. Tran, J. Li, L. Subramanian, and S.S. Chow, "Optimal Sybil-Resilient Node Admission Control," Proc. IEEE INFOCOM, 2011.

[6]. R.S. Peterson and E.G. Sirer, "Ant Farm: Efficient Content Distribution with Managed Swarms," Proc. Networked Systems Design and Implementation (NSDI), 2009.

[7]. E. Novak and Q. Li, "A Survey of Security and Privacy Research in Online Social Networks," Technical Report WM-CS-2012-2, College of William and Mary, 2012.

[8]. L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks," Proc. 18th Int'l Conf. World Wide Web (WWW '09), 2009.

[9]. B. Viswanath, A. Post, K.P. Gummadi, and A. Mislove, "An Analysis of Social Network-Based Sybil Defenses," Proc. ACM SIGCOMM, 2010.

[10]. J.R. Douceur, "The Sybil Attack," Proc. Revised Papers First Int'l Workshop Peer-to-Peer Systems (IPTPS '01), 2002.

[11]. Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "The Socialbot Network: When Bots Socialize for Fame and Money," Proc. 27th Ann. Computer Security Applications Conf. (ACSAC), 2011.

[12]. A. Mislove, M. Marcon, K.P. Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and Analysis of Online Social Networks," Proc. Seventh ACM SIGCOMM Conf. Internet Measurement (ACM/USENIX IMC), 2007.

[13]. A. Sala, L. Cao, C. Wilson, R. Zablit, H. Zheng, and B.Y. Zhao, "Measurement-Calibrated Graph Models for Social Network Experiments," Proc. 19th Int'l Conf. World Wide Web (WWW '10), 2010.

[14]. J. Davidsen, H. Ebel, and S. Bornholdt, "Emergence of a Small World from Local Interactions: Modeling Acquaintance Networks," Physical Rev. Letters, vol. 88, 2002.