Volume 4, Issue 4, April 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

HMAC Construction for Defense Mechanism for Sybil Attacks in Large Social Networks

S.Krishnaveni,
Reseach Scholar,
Department of Computer Science,
Hindusthan College of arts and Science,
Bharathiyar University,
Nava india, Coimbatore, India,

Dr. A.V.Senthil Kumar,
Director,
Department of MCA
Hindusthan College of Arts and Science,
Bharathiyar Unitversity,
Nava india,Coimbatore, India,

Abstract— Due to the development of WWW nowadays usage of peer-to peer networks have been widely increased and decentralized in several manner, several number of persons sharing their data to other person through social networks such as twitter, face book and orkut etc ,.These system are easily susceptible to Sybil attacks. In a Sybil attack, a malicious user hacks others user data through duplication of number of fake individuality. By controlling the malicious activities several methods have been proposed in earlier years through honest users to identification of Sybil users against online social networks. But still some of the Sybil attacks not found in the social network, in order to overcome this problem, in this study hash message authentication codes algorithm where key values are generated to each user in the graph to access network, against Sybil Defender. Based on the result of HMAC algorithm ,is well organized manner and is easily applied to huge social networks .The proposed HMAC algorithm easily identification Sybil attacks higher than the earlier Sybil attack methods ,it identifies Sybil attacks in each and every nodes in social networks is close to the hypothetically demonstrable subordinate bound.

Keywords— Sybil attack, Social network, Random walk, Keyed-Hash Message Authentication Code (HMAC), reputation systems, security, peer-to-peer(P2P) systems.

I. INTRODUCTION

In peer to peer environment in social networks permits users to share their services among different users in online efficient manner without any centralized management infrastructure. While transmission [1] and highly shareable storage devices [2] make use of this propose viewpoint include be anticipated, the not have of whichever essential manage more than characteristics such as Sybil attacks [3]: a small number of malevolent nodes can reproduce the occurrence of a extremely huge amount of nodes, to acquire over or interrupt explanation gathering to social networks .

Those types of attacks can be moderate through high and mighty the subsistence of a dependence ability, it becomes one of the rate level to identification of their fake results through conditions of rules for each user or some principle are specified to entire user in peer to peer network such as id number, social security number. Conversely, such a principle and rule determination of unauthorized user from networks, accepting the request to each and every user, in the social networks, as they force supplementary trouble on users.

These types of Sybil mechanism is categorized into centralized and decentralized ones. During centralized mechanism some nodes in the network which have highest authority is considered as best admission control node [3] ,it uses a rate level to each node in the network to identify the characteristics node by introducing fake created characteristic for each user ,that highly ensure the results of unauthorized user in the network and identification of best malicious node in well organized manner . These activities have been carried out through cryptography and public key certification mechanism as well as a guard of the proper reputation of the nodes establishes a very complicated difficulty in follow.

In the past years, usage of social network have been due to popularity and human being in multiple areas are connected by the majority commonly appointment sites on the web. These large usage of web sites need a specific methods to detect unauthorized uses that aims to detect malicious user nodes against social networks known as Sybil attacks be supposed to be well-organized and scalable. To perform this process proposed a graph based methods with cryptographic methods in distributed manners with hash tables [4] to control the usage of routing process in various paths in the networks systems. The well organized methods such as Sybil Guard [5] and Sybil limit [6] suggest the make use of OSN to moderate Sybil attacks. Since each and every user in the network have their own key to identify differentially and every one individuality mechanism on a particular mechanism. On the other hand, at what time Sybil attacks are initiate, the Sybil individuality effort on a particular workstation. When provide source uncontrollable tasks to a grouping of individuality within the threshold value specified through user, then if the user result is less considered as non Sybil attackers or else Sybil attackers. These type of resource consumption task have been carried out in earlier works [10]–[13] whether the selected user have possible amount of resources to identify Sybil attackers or not.

Generally Sybil attack task have been carried out through the representation of graph form for social networks, our proposed Sybil attack identification method is differs from normal methods since it uses a HMAC algorithm along with nodes for each user in the graph. We apply a set of Sybil attack to measure the results of HMAC-SI (Sybil attack identification) against social networks and measure result with increasing the number of user nodes concurrently. The proposed methods generate a hash key for each user in the social networks against Sybil attack defenses. For the reason that reasonableness is consequently significant for practical safety measures, chiefly in source controlled WSNs, identify number of Sybil attacks in the WSN with the intension of worst node is being founded for further investigation process.

II. BACKGROUND STUDY

In earlier work to detect Sybil attacks against P2P system was proposed by Douceur [7]. Similarly they used hierarchal model taxonomy level of security to detect attack and specified as many of Sybil attacks, to increase privacy level of social networks. Though these methods, may not clearly specify information to different types of attack specification [8]. To overcome the problem of detail analysis specification of Sybil attack types was proposed in [9].

Number of metrics also important to analysis result of Sybil attacks based on social networks with anti identification of attacks also in [14] and establish with the intention of those algorithms basically distinguish the public construction of truthful abuser. Following the procedures of these community methods , starts with like community based attack identification methods to increase the security level of Sybil attacks detection ,along with different location and different concepts their shared by user in the networks .Some of the work only focus on normal attack detection methods with centralized management ,other hand some of the work uses a signed based social network methods ,where conventional methods are used in globally and signed methods only applicable to some of social network only . Because the concept of community methods is moderately innovative, we are not confident whether it determination develop into a conventional solves the problem of social networks.

In earlier work [15] developed a distinct identities based social network methods to thwart attacks that is equivalent Sybil attacks [16], and it is applicable to WSN [17]. The methods might depends on making assuming that current user malicious user can enclose simply single network location, distinct in terms of its smallest amount latency in the direction of a set of encouragement.

In experimentation a result says that graph theory mechanism was used by earlier work is named as Sybil Guard. As an experimentation result if any one of the edges in the network is identified attack results based on boosting tree based mechanism [18] as the opposition generate further and additional Sybil nodes. It becomes one of the significant trust model used in WSN and PSP system. Many previous works [19-21] developed a trust management system for WSN and P2P systems based on earlier period doing well demonstrated experimentation between users in social networks. The management of trust result becomes very much stronger, which is fundamental in the direction of the success of Sybil Guard.

III. HMAC CONSTRUCTION FOR DEFENSE MECHANISM

In this work we consider a Sybil attack defender mechanism for social network; they consider two major steps to analysis and identification of Sybil user in the network. The major steps are Sybil identification algorithm, and HMAC construction algorithm to generate key values to Sybil user in the number of user in the social networks. In Sybil attack identification algorithm consider a graph G with edges and vertices$G(V,E)$, with a important node h, and a malicious node in the network of user is consider as output number of user in the network is consider as and outputs becomes whether user u is Sybil attacker or not .the number of user carried out through walk is defined as R. If the specific node in the user value is larger than the degree d_i then estimate the probability value of each user in the network(i,j), and move through the way of nearest neighbor j and it is equal to one. The initial step of identification of Sybil user is that construction of HMAC algorithm to users and generates a key for each user, then perform Sybil attack identification to each user in the network. Also, because of we assume that the length of Sybil user with maximum size in the social through the number of walk in the social network with user generated key from HMAC.

As shown in the algorithm 1 against Sybil attack identification in social networks along with key generated from HMAC, in order to determine whether a malicious nodes in social network is identified or not is known as Sybil user .In earlier work consider only number of frequency level to identify Sybil user, it becomes lesser identification Sybil attacks, Because keys are not generated to user. In this methods randomly perform number of walks and length of the users $l = 10$ or equal to l_{min}. The methods compare the result with user key values from HMAC and the number of occurrences of the frequency count of user time specification t along with deviation result of user in every number of tuple in the graph through random walk. If the earlier is lesser than the final through an quantity is higher than standard deviation and it is not equal to private key of the user, then we note the corresponding user a attacker or else normal user. The length of the algorithm is multiplied to 2 and perform the process repeatedly until it is larger than l_{max} .

Algorithm 1 :Sybil identification (G,U,KEYS ,Number of tuples)

$l = l_0$

While $l \leq l_{max}$ &key $\neq$ user k do

Perform R random walks with length l originating from u

M=number of nodes frequency at the specific time

The length of the user output $(l, \text{mean}, \text{standard deviation}, \text{user key from HMAC})$

If $\text{mean} - m > \text{std deviation} * \alpha \,|\text{key} \neq \text{userkey}$

Output u is Sybil

End the process
End if
$l = l * 2$
End while
Output u is honest
In the above Sybil attack identification method we additionally add key values from HMAC to enhance the security level. Hash based message authentication code is considered as one of the famous key encryption algorithm for secure user information .In HMAC system the keys are generated to each user in the social networks ,with user present in the network and hash them collectively.
The user in the network secret keys is generated and then perform Sybil attack identification algorithm as mentioned above. It is used to create authentication code to number of user to nodes in the social network. The authenticated code value is used to improve the security level of social network. The code value of hash function is created through usual hash function normal without any replacements of usual The user in the network secret keys is generated and then perform Sybil attack identification algorithm as mentioned above. It is used to create authentication code to number of user to nodes in the social network. The authenticated code value is used to improve the security level of social network. The code value of hash function is created through usual hash function normal without any replacements of usual constraints .The strength of HMAC algorithm is determined based on the hah value generated for user and original results of hash value. Although these HMAC is not considered to encrypt the message, it also identification of Sybil attacks in the social networks.

$$HMAC(K,U) = H(K \oplus OPAD)||H(K \oplus IPAD||U)$$

Where
H is a cryptographic hash function,
K is a secret key
,U is the number of user in the social network ,
‖ denotes concatenation,
⊕ denotes exclusive or (XOR),
$opad$ is the outer padding, and
$ipad$ is the inner padding for user in the social network given as input to HMAC[22] is shown in Figure 1.
n as input to HMAC[22] is shown in Figure 1.

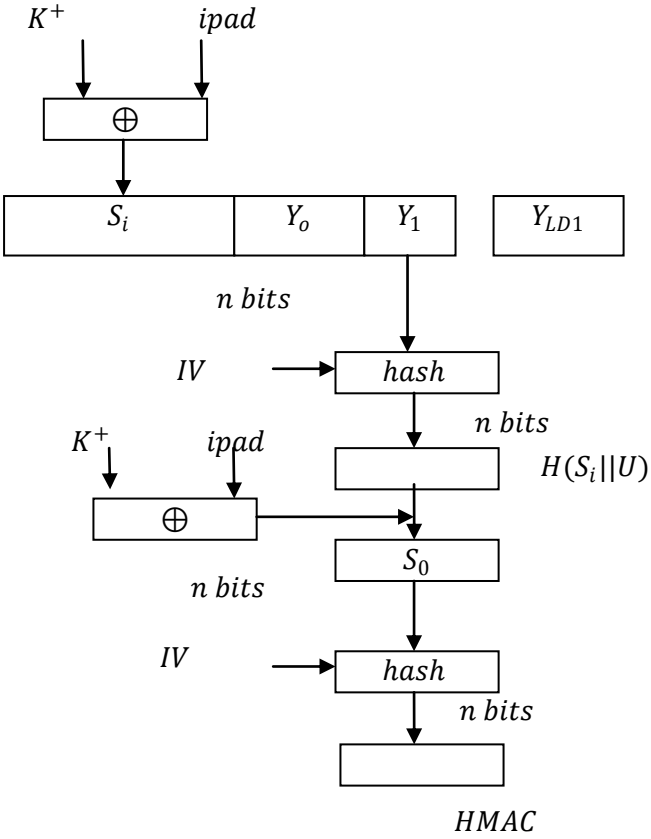

Figure 1: Structure of HMAC which implement the function

The results of HMAC authenticate code for social user in the network is binary values and it is equal to number of user length in the network .The security level of user is straightforwardly comparative to the essential hash function. If the security of the nodes in the network that is if the user is attacked by Sybil attack the hash function is considered as MD5

it becomes lesser security or else it is hash value is equal to SHA – 512 with highest security level with lesser number of attackers in the network. If the specific user is identified as Sybil attacker and need to perform Sybil attack identification, it requires more number of steps to analysis Sybil attacker in the social networks.

The specified hash authenticated code from HMAC user in the network carried out process of Sybil attack identification with key values results from through compression function which is whichever tradition or convention based algorithm [23]. From this way of process HMAC algorithm improves the security level of algorithm in the Sybil attack identification mentioned above which ensures authenticity of user, since a secret key is essential to replicate the confirmation system. The generated key for user in the social network with hash value can be used to extensively to determine Sybil attackers in the network. It provides original preservation of user in the social networks not consideration of accuracy results to any poverty

From this algorithm the node is identified as malicious node then detection can be estimated to find Sybil attack user population neighboring it. The community of user also identified in the graph with segregated regions, and there is rejection of nodes in the graph. The motivation of this algorithm also identification of Sybil user in the graph by dividing into many parts is considered specific region, to identify Sybil attack in social networks

IV. EXPERIMENTAL RESULTS

In this section, we evaluate the result of Sybil attacker user results against various social networks with datasets [24-25], correspondingly. Consider a larger dataset to estimate result of experimentation; have been used to estimate Sybil attackers result through HMAC and without HMAC algorithm. In this experimentation methods together both face book and orkut nodes share their information of one user node to another social nodes it the region, if both the user in the network have similar concept in the social network, and they are friends also in social networks.

To estimate results of Sybil attacks result against social networks, proposed system HMAC with Sybil attack identification algorithm and normal Sybil attack identification algorithm .measure the false and false negative rate .where false positive rate is defined as number of Sybil attacker correctly classified and false negative rate is defines as the percentage of the Sybil user identified as falsely Sybil user. These two rate are used to estimate result of hash message authentication code-Sybil attack identification (HMAC-SI) and Sybil attack identification (SI).

It is infeasible to observe each and every one the truthful nodes to obtain the accurate False Positive Rate (FPR) against HMAC-SI and SI. In testing experimentation we add attack to algorithm to measure how well the algorithm performs efficiently, contrast the quantity of Sybil attacks. For every value identified as Sybil user in the social network and it is separated into regions , the number of walks have been carried out in the social network simultaneously for each social network such as orkut and face book, correspondingly. The following Figure 2 shows the accuracy results of number of Sybil attack correctly identified and Figure 3 number of result falsely identified among hash message authentication code-Sybil attack identification (HMAC-SI) and Sybil attack identification (SI).

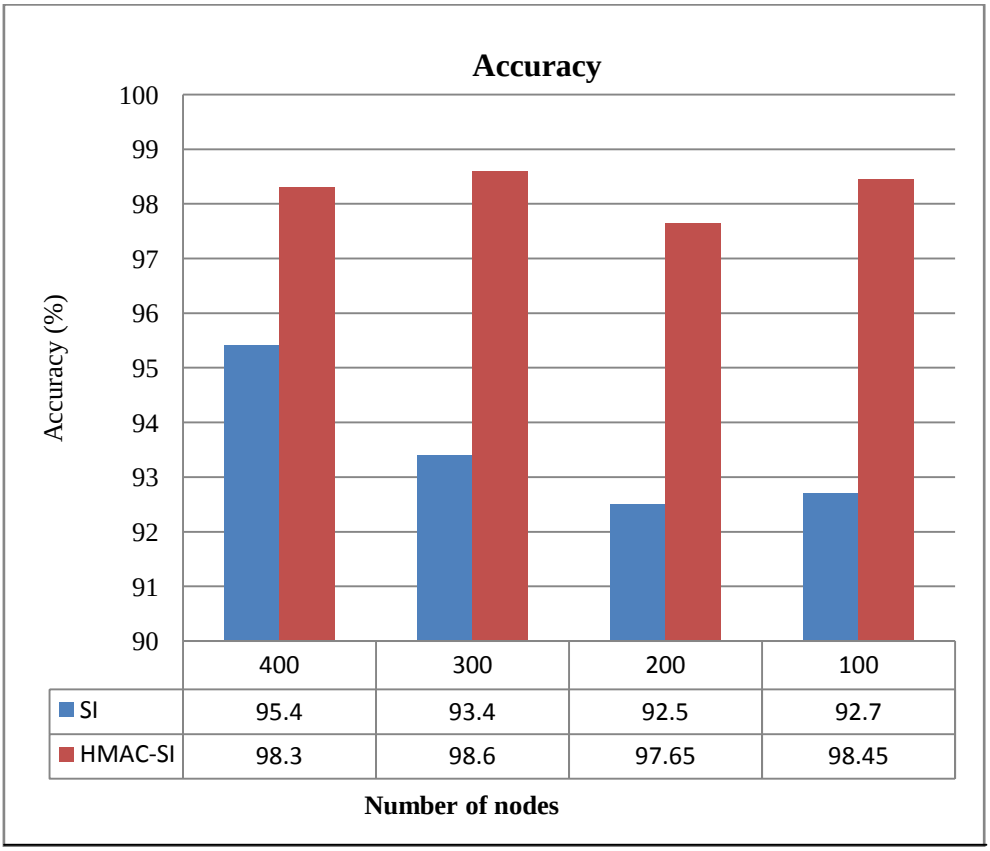

Figure 2: Accuracy of Sybil attacks detection.

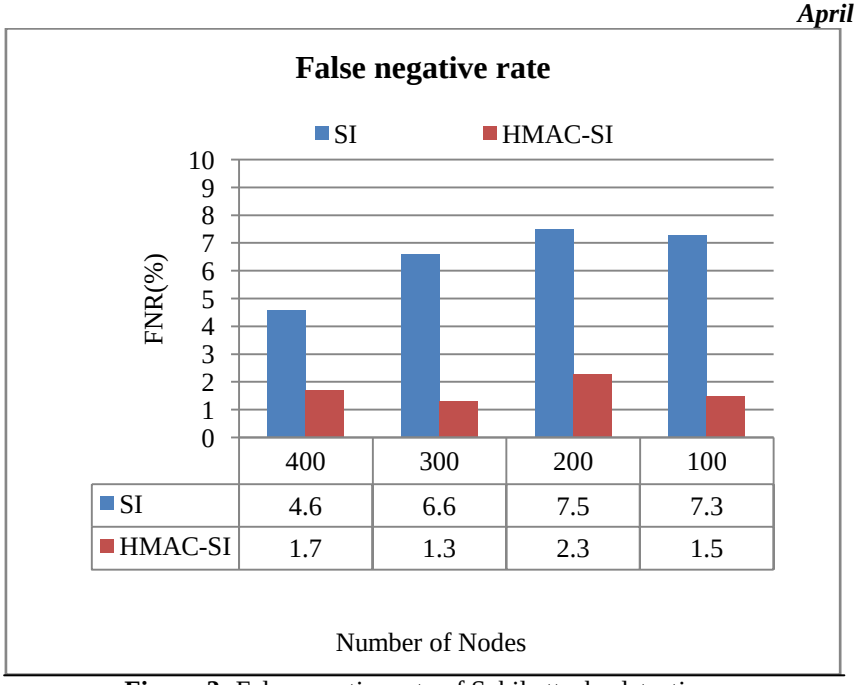

Figure 3: False negative rate of Sybil attacks detection.

V. CONCLUSION AND FUTURE WORK

In this paper presented a well efficient Sybil attacks identification algorithm for social networks with various topologies methods .The proposed system consists of two major steps Sybil attack identification algorithm and HMAC which generates hash key values for user in the social networks and it reduces the number of nodes whose suffered from Sybil attacks in social networks .Proposed HMAC-SI results demonstrated that HMAC-SI have identified more number of Sybil attack than SI approaches. Proposed methods are applied to social networks and results were measured through false positive rates and false negative rates ,it shows proposed HMAC-SI have higher percentage of false positive rate 98.6 % and less percentage of false negative rate 1.4 % with different sizes and structures.

In future work we apply these procedures into non anti Sybil attacks defend mechanism also with other methods and applications.

References

1. Stoica, R. Morris, D. Liben-Nowell, D. R. Karger, M. F. Kaashoek, F. Dabek, and H. Balakrishnan. **Chord: a scalable peer-to-peer lookup protocol for internet applications.** *IEEE/ACM Trans. Netw*., 11(1):17–32, 2003.
2. F. Dabek. **A cooperative file system**. *Master's thesis*, MIT, September 2001.
3. J. R. Douceur. **The sybil attack**. *In IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems*, pages 251–260, London, UK, 2002. Springer-Verlag.
4. G. Danezis, C. Lesniewski-Laas, M. F. Kaashoek, and R. Anderson**. Sybil-resistant dht routing**. *In ESORICS 2005: Proceedings of the European Symp. Research in Computer Security*, pages 305–318, 2005.
5. H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman. **Sybil guard: defending against sybil attacks via social networks.** *SIGCOMM Comput. Commun*. Rev., 36(4):267– 278, 2006.
6. H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao. **Sybil limit: A near-optimal social network defense against Sybil attacks.** *In IEEE Symposium on Security and Privacy*, pages 3–17, 2008.
7. Deng J. Han Y. Du, W. and P. Varshney, **A pairwise key pre-distribution scheme for wireless sensor networks,** *Proceedings of the 10th ACM conference on Computer and Communication Security*, 2003.
8. Tanya Roosta, S. P. Shieh, and Shankar Sastry, **Taxonomy of security attacks in sensor networks and counter measures**, *The First IEEE International Conference on System Integration and Reliability Improvements*, December 2006.
9. Seyit A. Camtepe and Bulent Yener, **Key distribution mechanisms for wireless sensor networks: a survey**.
10. C. Piro, C. Shields, and B. Levine, **Detecting the sybil attack in mobile ad hoc networks,** *in Proc. of IEEE Securecomm*, 2006, pp. 1–11.
11. B. Xiao, B. Yu, and C. Gao, **Detection and localization of sybil nodes in VANETs,** *in Proc. of ACM DWANS*, 2006, pp. 1–8.
12. Q. Zhang, P. Wang, D. Reeves, and P. Ning, **Defending against sybil attacks in sensor networks,** *in Proc. of IEEE ICDCS*, 2005, pp. 185–191.
13. M. Demirbas and Y. Song, **An RSSI-based scheme for sybil attack detection in wireless sensor networks,** *in Proc. of IEEE WoWMoM*, 2006, pp. 564–570.
14. B. Viswanath, A. Post, K. Gummadi, and A. Mislove, **An analysis of social network-based sybil defenses,** *in Proc. of ACM SIGCOMM*, vol. 40, no. 4, 2010, pp. 363–374.

15. R. Bazzi and G. Konjevod, **On the establishment of distinct identities in overlay networks,** *in Proc. 24th ACM Symp. Principles of Distributed Computing (PODC 2005), Las Vegas, NV*, Jul. 2005, pp. 312–320.
16. T. S. E. Ng and H. Zhang, **Predicting Internet network distance with coordinates-based approaches,** *in Proc. IEEE INFOCOM 2002*, New York, NY, Jun. 2002, pp. 170–179.
17. N. Sastry, U. Shankar, and D.Wagner, **Secure verification of location claims,** *in Proc. ACM Workshop on Wireless Security (WiSE'03),* San Diego, CA, Sep. 2003, 10 pp. 170–179.
18. G. Danezis, C. Lesniewski-Laas, M. F. Kaashoek, and R. Anderson, **Sybil-resistant DHT routing**, *in Proc. European Symp. Research in Computer Security (ESORICS 2005),* Milan, Italy, Sep. 2005, pp. 305–318.
19. A. Cheng and E. Friedman, **Sybil proof reputation mechanisms**, *in Proc. 3rd ACM SIGCOMM Workshop on Economics of Peer-to-Peer Systems (P2PECON-05), Philadelphia*, PA, Aug. 2005, pp. 128–132.
20. M. Feldman, K. Lai, I. Stoica, and J. Chuang, **Robust incentive techniques for peer-to-peer networks,** *in Proc. ACM Electronic Commerce (EC'04)*, New York, NY, May 2004, 10 pp.
21. M. Richardson, R. Agrawal, and P. Domingos, **Trust management for the semantic web,** *in Proc. 2nd Int. Semantic Web Conf. (ISWC2003),* Sanibel Island, FL, Oct. 2003, pp. 351–368.
22. **Cryptography and Network Security** *Chapter 12 – Hash Algorithms*. http://vlsi.byblos.lau.edu.lb/classes/ csc 736/ Notes/Lecture12.pdf
23. **DSA, Hash functions and HMACs** http://www.cs.rutgers.edu/~vinodg/teaching/spring-2008-cs442/slides/lecture6.pdf.
24. C. Wilson, B. Boe, A. Sala, K.P.N. Puttaswamy, and B.Y. Zhao, **User Interactions in Social Networks and Their Implications,** *Proc. Fourth ACM European Conf. Computer Systems (EuroSys),* 2009.
25. Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, **The Social bot Network: When Bots Socialize for Fame and Money,** *Proc. 27th Ann. Computer Security Applications Conf. (ACSAC)*, 2011

