MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

IDENTIFICATION AND PREVENTION OF FAKE IDENTITIES IN SOCIAL MEDIA

Shadaf J Warunkar, Nitin A Khandare, Jaihind D Mungle, Vishal V Shinde
Prof. Rohit Wagdarikar

Department of computer engineering,Dr. D. Y. Patil School of Engineering
Pune, India

Abstract: *Now Days online social networks such as Face book, Twitter, Google+, LinkedIn, have become extremely popular all over the world and play a significant role in people's daily lives. Due to open and anonymous nature of social sites the vulnerabilities on this social network are increasing, such as fake users also called as Sybil users. These kinds of malicious users can fabricate many dummy identities to target systems. So here we proposed a system. Which is a scalable defense system, which leverages user level activities such as friend acceptance, rejection? In this survey, our aim to give a comprehensive review of research related to user behavior in OSNs from several perspectives. First, we discuss social connectivity and interaction among users, Acceptance and rejections ratio are also important for that. Also, we investigate traffic activity from a network perspective.*

Friends invitation interactions among users as a social graph. Based on this social graph we proposed two key methods in order to detect fake identities that are fake users. Time Required to Browse and the time Gap Between the posting the status, sending SMS etc. Method is a voting-based Sybil detection and second is Sybil community detection to find other colluding Sybil around identified Sybil. In the second method we are using the global acceptance rate in order to detect the fake users. We are going to show the results in the form of global acceptance ratio of a particular user.

Keywords: *Online Social Network, Fake Identities, Global Acceptance ratio, Sybil attacks, social networks, social network-based Sybil defense, communities.*

1. INTRODUCTION

In the past decade a new kind of malicious behavior has been extensively studied. introduced as a Sybil attack. The attacker forges multiple identities, hence the name Sybil in order to subvert a system. For instance, a large number of Sybil can cast manipulated votes

to rig the outcome of a voting system. Sybil attacks are not only a threat in theory, but have also been observed in many real world.

In recent years, online social networks (OSNs) become huge and they are still growing throughout the world. Unfortunately, the openness and the tremendous growth of OSNs attract the interest of malicious parties. Sybil attack is one of the well-known and powerful attacks against OSNs. The malicious attacker generates a Sybil group consisting of multiple accounts (called Sybil users), and disguise them into different users. Sybil groups even collude together, build close relationships and generate communities. Sybil attacks are serious threats to OSNs: Multiple Sybil users are utilized to unfairly increase influence and power of target users. Moreover, Sybil attackers target OSNs as media to propagate spam Sybil attacks become increasingly dangerous as more people use OSNs as primary interfaces to the Internet. Various techniques were applied to identify Sybil users or spammers in OSNs, including rare social links between Sybil users and normal users honeypots manual identification and abnormal behavior Sybil users alone do not harm the system. What is really dangerous is that multiple Sybil users are controlled together to form a Sybil group some research took initial steps and designed algorithms to detect Sybil groups Further explores the negative different relationships (e.g., in the form of rejected friend requests) among users, as Sybil have more distrust relationships than trust ones with real users. However, this feature cannot be directly applied because attackers could obfuscate their Sybil from the detector by generating many fake trust relationships among Sybil.

2. LITERATURE SURVEY

2.1 Exploiting Mobile Social Behaviors for Sybil Detection:

In this research work they have proposed a social-based mobile Sybil detection scheme to detect four levels of Sybil attackers with different attacking capabilities. They have investigated mobile user's pseudonym changing behaviors compared with that performed by Sybil attackers, and utilized contact statistics as the criteria of pseudonym changing for mobile Sybil detection. The security analysis demonstrates that the SMSD can resist four levels of Sybil attackers, while the extensive trace based simulation can validate the detection accuracy of the SMSD [1].

2.2 Malicious Behavior on OSN:

The usage of OSNs introduces numerous security and privacy threats. For instance, as a user needs to interact with other users through an OSN service provider, its activities and uploaded data can be tracked and stored by the OSN service provider. These data (photos, articles, public posts, private messages, etc.) may be leaked to a third party without the user's explicit authorization, even when the user regards some of these as confidential. Moreover, Sybil attacks are very common in OSNs, as a user can register multiple fake accounts maliciously. These fake accounts can perform various malicious activities including spamming, obtaining privacy contact lists, misleading crowd-sourcing results, and so on. Besides those, list several other attacks such as re-identification and de-anonymous of anonymous OSN data, fetching personal data through untrusted third-party applications,

cross-site profile cloning, social spamming, and phishing. Due to space limitation, this survey mainly focuses on malicious behavior in OSNs, including spam and Sybil attacks.

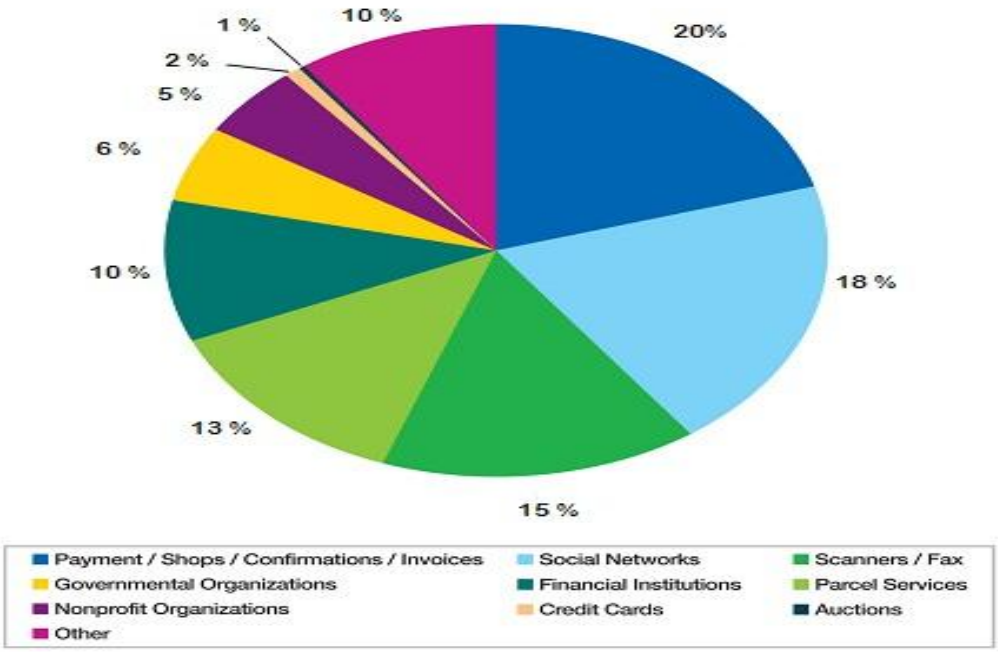

Fig.1: Attacking area [2]

2.3 Sybil Attacks and Their Defenses in the Internet of Things:

Here they have provided a survey of Sybil attacks and their defense schemes in IOT. Specifically, they have defined three types of Sybil attacks in the distributed IOT and presented some Sybil defense schemes with the comparison. The differential characteristics, including social structures and behaviors, between Sybil attackers and normal users could facilitate the Sybil defense. In addition, MSD can leverage mobile network features, wireless channel characteristics, and cryptography to resist Sybil attackers.[2]

Disadvantages:

They have some disadvantages research issues such as Sybil defense in MSNs, tradeoffs between privacy and learning in Sybil defense, and cooperative Sybil defense.

2.4 Combating Friend Spam Using Social Rejections:

Here they contribute to fight against fake accounts that act as friend spammers in Face book-like symmetric OSNs, driven by the observation that even well-maintained fake accounts inevitably have their friend requests rejected by legitimate users end. they propose Rejecto, a system that detects accounts that send out unwanted friend requests. Rejecto augments the social graph with social rejections, and seeks the minimum aggregate acceptance rate cut. With this formulation, our system is able to uncover friend spammers in a manipulation-resistant way. We evaluate Rejecto through extensive simulations that are driven with real-world OSN samples. We also evaluate our parallel implementation on an

EC2 cluster evaluation results show that Rejecto is effective in a broad range of scenarios.[3]

2.5 Trust in Social Networks by Three-Valued Subjective Logic:

Three-valued subjective logic is proposed to compute the interpersonal trust between any two persons who have not had interactions before. 3VSL introduces posteriori uncertainty space to store the evidences distorted from certain spaces as trust propagates, and priori uncertainty space to control the evidence size as trusts combine. We also discover the differences between distorting and original opinions, i.e. original opinions are so unique that they can be reused in trust computation while distorting opinions are not. We validate 3VSL both in theory and real world evaluation. The results indicate that 3VSL is sound and can be applied in computing trust with high accuracy. [4]

Disadvantages:

Bayesian analysis will be integrated to make 3VSL is not able to from multiple sources.

OSN site	No. of users
Facebook	1.01 billion (Oct. 2012)
Twitter	500 million (Apr. 2012)
Google+	400 million (Sep. 2012)
LinkedIn	175 million (Jun. 2012)
Foursquare	25 million (Sep. 2012)

Table.1: Users of Popular OSN [12]

In Table.1 Shows that Popularity of Different OSN and Number of user on OSN Site and from that we can't find the how many users are Sybil users. To find that Sybil users we proposed our system.

3. SYSTEM IMPLEMENTATION

We now describe the design of our proposed work, which considers the fake user detection as a vote aggregation problem. In this application a link of the friend invitation graph means that one node casts a certain number of votes for the other users. The vote value is determined by the sign of link. For each node user, Voters guarantees that votes are mainly collected from real users by pruning the collusion votes among fake users. Further the system identifies the fake user for which the majority of votes are negative.

Type	Edge
Friendship graph	Friendship between users
Interaction graph	Visible interaction, such as posting on a wall
Latent graph	Latent interaction, such as browsing profile
Following graph	Subscribe to receive all messages

Table.2: Different type of Social Graph on OSN

3.1 Social Graph Based on Request Acceptance & Rejections:

On OSN Different kinds of social graphs can reveal how users connect and interact with each other. However due to the limited information that the graph can represent, various types of users' activities cannot be characterized e.g., time duration of browsing a profile. An observation from network operators can monitor such information easily, and interpret how users use OSNs better. Furthermore, for ISPs, they have strong incentive to get better understanding of how the traffic pattern between end users and OSN sites will evolve, and take optimization actions according to the distribution and activities of OSN users. In this section, we review OSN user behavior study from the perspective of network traffic analysis. And find the ratio of friend request acceptance and rejections.

3.2 Trust based vote assignment:

The main aim of trust-based Votes assignment is to assign low vote capacity to fake users that can be useful to limit the number of votes that fake users could cast for each other. In order to carry out this functionality we first select some trusted users as seeds Vs, and through this seeds propagate the vote capacity to others along the links of friend invitation graph G(V;E). As Fake users region has a limited number of in-links we can say that the total vote capacity entering the Sybil region is constrained.

3.3 Global Weight Aggregating:

The first method of Vote assignment gives low vote capacity to not only Fake users but also non-popular real users with few incoming links. So to overcome this we introduce the global vote aggregating phase to get the global acceptance rate $p(u)$ of a node u. In this method it leverages the sign of outgoing links (i.e., the user feedback) for higher accuracy. Fake users have a higher percentage of negative links to real region so we can identify the fake users.

3.4 Technology used:

We are developing our project as a web based application using Open Source Java technology; java is an more secure & in Net beans IDE and MYSQL as a database.
Both the approaches presented above are described through an algorithm show below which has two phases Vote Assignment and Vote Aggregating.

VOTERS-D(*G; Vs*)

- if *u* ϵ *Vs* then ;vote assignment
  I(*u*) ← *N*=| *Vs*|
- else
  I(*u*) ← 0;
- end if
- while Δ > *ϵ1* do
- for *u* ϵ *V* do
- $U(u) = \mathrm{d}.\sum_{v:(v,\mathcal{U})\epsilon \mathrm{E}} \frac{\vartheta(v)}{\omega(v)} + \big((1-\mathrm{d}).\mathrm{I}(u)\big)$
- end for
- end while
- *p*(0) ←0:5; ;vote aggregating
- while Δ > *ϵ2* do
- for *u 2*ϵ *V* do
- $\mathrm{P}(u) = \frac{\sum v:(v,\mathcal{U})\epsilon\, E + \vartheta(v).p(v)}{\sum v:(v,\mathcal{U})\epsilon\, E\vartheta(v).p(v)}$
- *p* ←WilsonScore();
- end for
- end while
- end procedure

4. CONCLUSION

In this survey papers, we study user behavior in OSNs from four different perspectives-connection and Interaction, traffic activity, social behavior and malicious behavior user interactions of initiating and accepting links to defend against fake users. From this system we can guaranty that our proposed work, will limit the number of requests Sybil's can send to real users. Our evaluation shows that our system able to detect real fake users with high precision and outperforms traditional ranking systems.

REFERENCES

[1]. Kuan Zhang, Xiaohui Liang, Rongxing Lu, Kan Yang IN "Exploiting Mobile Social Behaviors for Sybil Detection" in the 2015 IEEE conference,2007.

[2]. Kuan Zhang, Xiaohui Liang, in "Sybil Attacks and Their Defenses in the Internet of Things" in IEEE internat of things journal, vol.1, no 5, October 2014

[3]. Qiang Cao Michael Sirivianos, Xiaowei Yang Kamesh Munagala in "Combating Friend Spam Using Social Rejections".

[4]. Guangchi Liu,Qing Yang, Honggang Wang, Xiaodong Linz and Mike P in "Assessment of Multi-Hop Interpersonal Trust in Social Networks by Three-Valued Subjective Logic".

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

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

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

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

[9]. J. Xue, Z. Yang, X. Yang, X. Wang, L. Chen, and Y. Dai, "Votetrust: Leveraging friend invitation graph to defend against social network sybils," in Proc. of INFOCOM, 2013.

[10]. J. Jiang, C. Wilson, X. Wang, P. Huang, W. Sha, Y. Dai, and B. Y. Zhao, "Understanding latent interactions in online social networks," in Proc. of IMC, 2010.

[11]. L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: automated identity theft attacks on social networks," in Proc. of WWW, 2009.

[12]. [12] Understanding User Behavior in Online Social Networks: A Survey - 2013 IEEE