International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

# Fake Profile Identification in Social Network

**Santosh Kumar Mehta, L.N. Padhy, Rajesh Kumar Gupta**
Department of CSE, Konark Institute of Science and Technology, Bhubaneswar, Odisha, India

## ABSTRACT

In present generation, the social life of everyone has become associated with the social networking Sites. The time spent on sites like Facebook or LinkedIn is constantly increasing at an impressive rate. At the same time, users populate their online profile with lots of information that aims at providing a complete representation of themselves. But with their rapid growth, it creates many problems like fake profiles, online impersonation. Fake account means malicious users of social networks to send spam, commit fraud. A single malicious actor may create thousands of fake accounts in order to scale their operation to reach the maximum number of legitimate members. In this paper focus is made on social networks for detection of fake profile. An attempt has been made to analysis various existing techniques that include comparison in perspective of various applications mapping various performance parameters.

**Keywords:** Online Social Networks (OSN), Facebook Immune System (FIS), phishing, Social Networking Sites (SNS).

## I. INTRODUCTION

A social networking site is a website where each user has a profile and can keep in contact with friends, share their updates, meet new people. These Online Social Networks uses web2.0 technology, which allows users to interact with each other. These social networking sites are growing rapidly and changing the way people keep in contact with each other. The online communities bring people with same interests together which makes users easier to make new friends.

Online Social Media such as Facebook, Twitter, or LinkedIn, allow for users to present themselves as an online profile, using these profiles, users are able to setup variety online social relationships in a popular way. Due to the open nature of OSNs, users can appear in redundant identities. Hence, verifying users' identities is one of the critical issues from the security and privacy point of view. To set up any social relationships in an authenticated fashion, the users must authenticate their identities to each other in order to prevent building fake communications on a large scale. The current way of authenticating user identities in OSNs is not enough to prevent fake profile creation, such that the single user can represent his identity with multiple profiles without any effective identity verification process. This vulnerability enables the attackers to create a variety of fake profiles for attacking the online social System.

Profiling Attack through which the adversary tries to gather information about OSN activities. Retrieval and Analysis attack is another malicious behavior, which targets multimedia information such as images, videos, audios, etc. This attack is followed by subsequent analysis as a Reverse Engineering Attack (RSE) , by which the attacker seeks to trick the victim into contacting with the hacker freely. Sybil attacks are one of the most prevalent and practical attacks against OSNs platforms, in this attack, the adversary seeks to impersonate the real users' identities across OSN via creating several fake accounts known as Sybil accounts to obtain the trust of a specific user or a specific community unfairly. Unfortunately, OSNs platforms have not strong authentication mechanisms for protecting users' profiles against Sybil profile attack except for the traditional mechanisms, such as CAPTCHA, which is routinely solved by dedicated workers for pennies per request. Although the researchers introduced several methodologies and approaches for detecting Fake profiles, but it is still a

hard challenge. For example, some machine learning algorithms are proposed, but they do not provide the desired effectiveness and accuracy to detect fake profiles. Other researchers tried to solve this problem using Social Graph Topology and its properties , but there is a little evidence for depending on these approaches for detecting fake profiles in OSNs. Crowd sourcing, is a different approach for identifying Fake profiles but also it doesn't provide the effective and accurate solutions as it depends on a human-based account verification scheme. In this thesis I am try to detect of fake profiles with active leaning from the feedback of the result given by the classification algorithm.

## II. REVIEW OF LITERATURE

Fake profiles are the profiles which are not genuine i.e. They are profiles of persons who claim to be someone they are not, doing some malicious and undesirable activity, causing problems to the social network and fellow users.

Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password.

If a criminal manages to hack or socially engineer one person's email password they have access to that person's contact list–and because most people use one password everywhere, they probably have access to that person's social networking contacts as well.

Once the criminal has that email account under their control, they send emails to all the person's contacts or leave messages on all their friend's social pages, and possibly on the pages of the person's friend's friends.

A phisher sends an e-mail, IM, comment, or text message that appears to come from a legitimate, popular company, bank, school, or institution.

These messages usually have a scenario or story. The message may explain there is a problem that requires you to "verify" of information by clicking on the displayed link and providing information in their form. The link location may look very legitimate with all the right logos, and content. Because everything looks legitimate, you trust the email and the phony site and provide whatever information the crook is asking for. These types of phishing scams often include a warning of what will happen if you fail to act soon, because criminals know that if they can get you to act before you think, you're more likely to fall for their phish.

The email claims to be from a lottery, or a dead relative, or the millionth person to click on their site, etc. In order to give you your winnings you have to provide *information about your bank routing* so they know how to send it to you, or give your address and phone number so they can send the prize, and you may also be asked to *prove who you are* often including your Social Security Number. These are the greed phishes where even if the story pretext is thin, people want what is offered and fall for it by giving away their information, then having their bank account emptied, and identity stolen.

The use of someone else's name to send email, post material, create social networking accounts, or contact other people in any way is called *online impersonation* or *e-personation*, and parents should be aware of how online impersonation can be used to harass adults and children. Since there's currently no way for most online platforms to verify account information, it's easy to make an email or social networking account in someone else's name. Using someone else's name is a powerful tool for damaging reputations and harassing others. An account made under someone else's name, especially if it's a trusted individual, can be used for everything from cyber bullying to phishing to extortion.

Most attackers are in it to make money. They make money by distributing unwanted ads (spam) or capturing accounts they can reuse or resell (phishing). Attackers need resources to make a profit - fake

accounts, real accounts, IP addresses, email accounts, and computing power. All these assets can have a significant cost associated with them, and an attack, like any business venture, needs profit to keep going. An effective response quickly limits the impact of an attack and vastly increases costs for any malicious attacker.

Attackers will try to use Facebook accounts, Pages, Groups, Events, and Apps to steal login information, spam people, and ultimately make money. They need email accounts, cookies, and a wide range of IP addresses to circumvent reputation-based defenses. Additionally, they use phone numbers, stolen credit cards, and CAPTCHA solutions in an attempt to circumvent authentication checks. All of these assets are scarce and not free for the attacker. Some assets are more valuable than others, and by confiscating, deactivating or disabling these assets we can sufficiently raise the costs of an attack so it is no longer profitable.

An attack is stopped by blocking its spread and destroying its assets. Ideally, as with most crime, once the activity is no longer profitable, the people behind it move on to some form of legitimate economic activity like teaching computer science or waiting tables. To block and destroy we employ a number of techniques from statistics and computer science, and we do it on a large scale.

The Immune System analyzes every action on the site as it happens, to determine its threat level, and decide how to respond. To make this decision it looks at the reputation of the cookie, IP address, and a number of other factors.

Defeating attacks relies on quick response times. If we can detect a new attack quickly, we can seriously limit its damage. Blocking bad actions directly cuts the spread of the attack. Destroying assets raises the cost for attackers. The importance of response time means that system performance plays just as much of a role as the algorithms themselves.

## III. METHODS AND MATERIAL

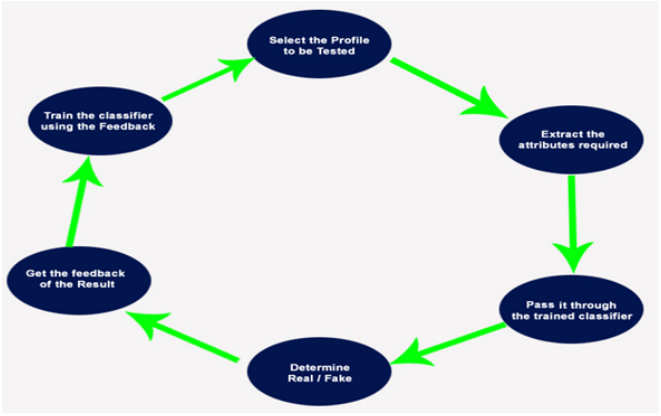


**Figure 1:** Framework for detection of fake profiles and learning

The framework shows the steps that need to be followed for identifying of fake profile with active leaning from the feedback of the result. The social networking companies can easily implement this framework.

1. The selection of the profile that needs to be tested.
2. When the profile is selected, select suitable attributes (features) on which the classification algorithm is implemented.
3. The attributes gained is passed to the trained classifier. The classifier gets trained regularly, when new training data is feed into the classifier.
4. Fake or real Profile is determined by the classifier.
5. The classifier may not judge 100% accuracy of the profile. So, the feedback of the result is necessary. For example, if the fake profile is identified, social networking site sends notification to that profile to submit their identification. If the valid identification is provided by the profile owner then feedback is sent to the classifier that the profile was not fake.
6. The repetition of process occurs several times with different profile, the number of training data increases and the classifier becomes more and more accurate in predicting the fake profile.

Classification is the process of learning a target function f that maps each records, x consisting of set of attributes to one of the predefined class labels, y. A classification technique is a approach of building classification models from an input dataset. This technique uses a learning algorithm to identify a model that best fits the relationship between the attribute set and class label of the training set. The model generated by the learning algorithm should both fit the input data

correctly and correctly predict the class labels of the test set with as high accuracy as possible. The key objective of the learning algorithm is to build the model with good generality capability. The figure 2 shows the general approach for building a classification model.

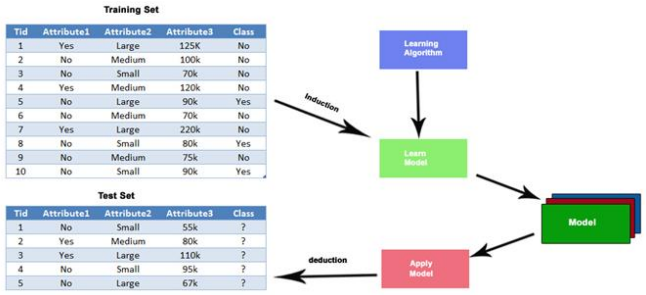


**Figure 2:** General Approach for Building a Classification Model

## IV.CONCLUSION

We have given a framework using which we can detect fake profiles in any online social network with a very high efficiency as high as around 95%. Fake profile detection can be improved by applying NLP techniques to process the posts and the profile. Thus, we can analyses the all needed attributes from the users that help us to recognize their profiles are real or fake.

## V. REFERENCES


[1]. T. Stein, E. Chen, and K. Mangla. Facebook immune system. In Proceedings of the 4th Workshop on Social Network Systems, SNS, volume 11, page 8, 2011.

[2]. A. Wang. Detecting spam bots in online social networking sites: a machine learning approach. Data and Applications Security and Privacy XXIV, pages 335-342, 2010.

[3]. C. Wagner, S. Mitter, C. K'orner, and M. Strohmaier. When social bots attack: Modeling susceptibility of users in online social networks. In Proceedings of the WWW, volume 12, 2012.

[4]. G. Kontaxis, I. Polakis, S. Ioannidis, and E.P. Markatos. Detecting social network profile cloning. In Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on, pages 295-300. IEEE, 2011.

[5]. S. Krasser, Y. Tang, J. Gould, D. Alperovitch, and P. Judge. Identifying image spam based on header and file properties using c4. 5 decision trees and support vector machine learning. In Information Assurance and Security Workshop, 2007. IAW'07. IEEE SMC, pages 255-261. IEEE, 2007

[6]. H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B.Y. Zhao. Detecting and characterizing social spam campaigns. In Proceedings of the 10th annual conference on Internet measurement, pages 35-47. ACM, 2010.

[7]. Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia. Who is tweeting on twitter: human, bot, or cyborg? In Proceedings of the 26th Annual Computer Security Applications Conference, pages 21-30. ACM, 2010.

[8]. S. Krasser, Y. Tang, J. Gould, D. Alperovitch, and P. Judge. Identifying image spam based on header and file properties using c4. 5 decision trees and support vector machine learning. In Information Assurance and Security Workshop, 2007. IAW'07. IEEE SMC, pages 255-261. IEEE, 2007.

[9]. G.K. Gupta. Introduction to Data Mining with Case Studies. Prentice Hall India, 2008.

[10]. Rajan Chattamvelli. Data Mining Methods. Narosa, 2010.

[11]. Spies create fake facebook account in nato chief's name to steal personal details, http://in. news.yahoo.com/spies-create-fake-facebook-account-nato-chiefs-name-114824955. html.

[12]. Man arrested for uploading obscene images of woman colleague, http://www.ndtv.com/ article/andhra-pradesh/man-arrested-for-uploading-obscene-images-of-woman-colleague-173266.

[13]. Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu. The socialbot network: when bots socialize for fame and money. In Proceedings of the 27th Annual Computer Security Applications Conference, pages 93-102. ACM, 2011.

[14]. S. Nagaraja, A. Houmansadr, P. Piyawongwisal, V. Singh, P. Agarwal, and N. Borisov. Stegobot: A covert social network botnet. In Information Hiding, pages 299-313. Springer, 2011.

[15]. M. Huber, M. Mulazzani, and E. Weippl. Who on earth is mr. cypher: Automated friend injection attacks on social networking sites. Security and Privacy-Silver Linings in the Cloud, pages 80-89, 2016.

[16]. T. Stein, E. Chen, and K. Mangla. Facebook immune system. In Proceedings of the 4th

Workshop on Social Network Systems, SNS, volume 11, page 8, 2011.

[17]. Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu. The socialbot network: when bots socialize for fame and money. In Proceedings of the 27th Annual Computer Security Applications Conference, pages 93-102. ACM, 2011.

[18]. C. Wagner, S. Mitter, C. K'orner, and M. Strohmaier. When social bots attack: Modeling susceptibility of users in online social networks. In Proceedings of the WWW, volume 12, 2012.

[19]. G. Kontaxis, I. Polakis, S. Ioannidis, and E.P. Markatos. Detecting social network profile cloning. In Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on, pages 295-300. IEEE, 2011.

[20]. A. Wang. Detecting spam bots in online social networking sites: a machine learning approach. Data and Applications Security and Privacy XXIV, pages 335-342, 2010.

[21]. H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B.Y. Zhao. Detecting and characterizing social spam campaigns. In Proceedings of the 10th annual conference on Internet measurement, pages 35-47. ACM, 2010.

[22]. Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia. Who is tweeting on twitter: human, bot, or cyborg? In Proceedings of the 26th Annual Computer Security Applications Conference, pages 21-30. ACM