DETECTION OF FAKE PROFILE IN SOCIAL MEDIA

Jyoti Singh and Mohammad Zunnun Khan

Department of Computer Science and Engineering Integral University, Lucknow

Abstract: Online social networks are increasingly influencing how individuals interact with each other by exchanging their private and professional data. The social network is currently a common way to communicate with others that are spread across a variety of locations around the globe. When we speak about social networking then we can say that by sending them a request or readily sharing data with each other, anyone can readily make friends. An individual user can have numerous accounts at various social networking locations to maintain in contact with their colleagues. Most social network users are unaware of the multiple kinds of safety problems or assaults such as privacy violations, identity theft, etc. Anyone can readily generate a fake profile with a true user's name and the other users will think it's an authentic profile, they might acknowledge the fake friend application. It makes the network somewhat confusing and frustrating. In this document, we address fake profiles and the suggested scheme that can detect comparable fake social network profiles that can make it simpler to connect with others in a secure and effective way. . People are like to spend their much time on the social networking site. A vast amount of information is being developed and divided around the globe via social networks. These interests have led to unlawful users engaged in fraudulent activity against social network users. This paper focuses on the literature assessment of state-of-the-art social media studies that detect false profiles. False identities play a significant role in sophisticated persistent threats and are also engaged in other malicious operations. This paper focuses on the literature review of state-of - the-art studies directed at identifying false profiles in social media. The approaches to identifying fake social media accounts can be categorized into methods directed at analyzing individual accounts and approaches capturing coordinated operations spanning a large group of accounts. The paper sheds light on the role of fake identities in sophisticated constant threats and includes the above approaches to identifying fake social media accounts.

Keyword: Privacy violation, fake profile, fake identities, social network analysis

I. INTRODUCTION

Social networking site is a website where each user has a profile and is able to keep up with friends, share updates and meet new stakeholders. The social networks online use the technology web2.0, which enables users to communicate. These social networking websites grow quickly and change the contacts between individuals. The online community brings together individuals with the same interests, facilitating user friendships. Social impact Everybody's social life has been linked to internet social networks in the current generation. These sites have dramatically altered our way of living in society. New friends and updates have become simpler to keep in touch with. Online social networks influence science, education, grassroots organization, work, company, etc. These internet social networks have been studied by researchers to see their effect on the individuals. Teachers can readily reach their learners in a pleasant setting, educators now familiarize themselves with these websites that bring online classroom pages, do homework, talk, etc. which greatly enhances their schooling. In spite of all the advantages such social sites have their own disadvantages as well, in a certain way they pose threat to unvigilant individuals. Attacks such as phishing, spoofing, spamming, etc. have become really common. Measures

should be taken to either control or detect such attacks. The individuals of a platform should be prudent enough to understand which people can be added to their social media accounts for this purpose the social media sites should provide certain filtering criteria which will in turn weed out the fake or suspicious accounts. Many researches have been carried out for the same [1], [2], [3], and [4] that do a in depth study about fake profile detection.

II. Fake Profiles

Profiles which are not real, i.e. profiles of people who pretend to be someone they do not, perform some malicious and unwanted work, cause social network issues and fellow users, are termed as fake profile. Fake social media accounts are becoming a problem not just for society as a whole, but also for companies. They can be used to wage war against a company for shady reasons, and it can turn into a nightmare for the target company when it happens.

Each user has their own identity that separates them from other users, such as name, I’d evidence, passport that includes date of birth, fingerprint etc. Online casual groups (Online Social Networks) empower and energize outsiders (apps) to enhance client encounters at these phases. Such improvements integrate intriguing or engaging techniques of conveying to internet companions and various exercises, such as playing recreations or tuning in to melodies.[5]

Today, individuals around the globe depend on OSNs to share knowledge, views and experiences; to seek data and resources; and to develop private links. However, the same characteristics that make OSNs precious to normal individuals also make them targets for different types of violence.[6] For example, the large audience on a single platform is a prime target for spammers and scammers, and the platform's trustworthiness may make the targets more likely to fall for scams. The application can spread spam by reaching extensive amounts of customers and their companions;

1) The request may obtain information from customers close to home, such as email address, primary residence and sexual orientation ;
2) The request may be "replicated" by making known various vindictive apps.
3) A typical situation for using false identities is to use social media platforms to impersonate someone or to create a false identity in order to build confidence With the target, this is then utilized.
4) For gathering further information for a spear phishing attack.[7]
5) Mounting a spear phishing attack or for direct interaction to get interest information.[8]

In the sequel, we considered accounts initially authentic, but later compromised as fake accounts. We also call fake accounts that contain private data that does not belong to the individual who produced this account. If the account includes personal details invented, it is called a fake account.[9]

III. Detection of Fake Profile

Fake identities in social media are often used in APT instances, both to collect pre-attack intelligence and to build confidence and offer malware or a link to it. Such false identities are also used in other kinds of malicious activity. To combat these activities, a significant body of research has so far focused on the timely and accurate detection of the presence of a fake identity in social media.

A. Small Scale Use of False Social Media Identities

A number of False Account Detection approaches rely on the evaluation of individual social network profiles in order to identify features or a mixture that helps to distinguish between lawful and fake accounts.[10-15] Specifically, different characteristics are obtained from the profiles and messages, and then machine learning algorithms are used to construct a classifier capable of identifying fake accounts.

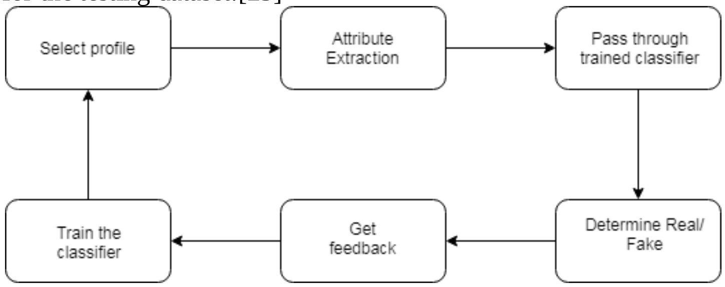
B. **Large-scale use of fake social media identities** A particular sort of large-scale fake account creation campaign is referred to as crowdturfing, a term representing a merger of two other terms, astroturfing (i.e. sponsored data dissemination campaigns disguised as spontaneous movement) and crowdsourcing. Thus, crowdsourcing is malicious.[16]

IV. Proposed Work

Overview

Each profile (or account) in a social network contains loads of data such as gender, friend no., comment no., education, job etc. Some of this data is private and some is public. Since personal data is not available, we have used only government data to determine the false profile in the social network. However, if our suggested system is used by the social networking businesses themselves, they can use the profile's personal data for identification without breaking any privacy issues.[17] We have regarded these data as characteristics of a profile for the classification of fake and true profiles.The steps we have followed to detect fake profiles are as follows:-

1. First, all the characteristics on which the classification algorithm is implemented are chosen. Proper care should be taken when selecting characteristics such as characteristics should not be dependent on other characteristics and those characteristics should be selected which can boost classification effectiveness.[18]
2. After adequate choice of characteristics, the data set of earlier recognized fake and true profiles is required for the training purpose of the classification algorithm. We have produced the actual profile dataset, whereas the fake profile dataset is supplied by Barracuda Labs, a privately held company that provides safety, networking and storage solutions based on network appliances and cloud services.[19]
3. The characteristics chosen in step 1 must be extracted from the profiles (fake and real).For social networking firms that want to enforce our system do not need to follow the scrapping method, they can readily remove the characteristics from their database. We applied the scrapping of the profiles as no social network dataset is publicly available for the purpose of detecting the fake profiles.[20]
4. After that, the fake and true profile datasets are ready. From this dataset, 80 percent of both profiles (true and fake) are used to prepare a training dataset and 20 percent of both profiles are used to prepare a test dataset. We find the efficiency of the classification algorithm using a training dataset containing 922 profiles and a test dataset with 240 profiles. [21-24]
5. The training dataset is fed to the classification algorithm after preparing of the training and testing dataset. It learns from the training algorithm and is supposed to provide the right class levels for the testing dataset.[25]



1. First, all the characteristics on which the classification algorithm is implemented are chosen. Proper care should be taken when selecting characteristics such as characteristics should not be dependent on other characteristics and those characteristics should be selected which can boost classification effectiveness.[26]

2. After adequate choice of characteristics, the data set of earlier recognized fake and true profiles is required for the training purpose of the classification algorithm. We have produced the actual profile dataset, whereas the fake profile dataset is supplied by Barracuda Labs, a privately held company that provides safety, networking and storage solutions based on network appliances and cloud services.[27]

V. IMPLEMENTATION OF THE TOOL

1. collect information about u and v

- Are family(u,v)
- Common comments(u,v)
- Common friends
- Share like and post

2. commonstrength(u,v)=cs(u,v)=commonfriends(u,v)+commoncomments+are family+ share like and post

3. cs-Average-precision(p)=∈{user∈ user||friend(user)}pu(p)/|{user∈ user||friends||friends(user)|≥p}

4. Collect all the features of the account

5.classify the features of user by NB

6. C[] ← received the classify result in cluster

array

7. Process the c[n] in another classifier and return ranking of account.

8. If ranking is less than 4 then it is fake account.

VI. OUR APPROACH FOR DETECTING FAKE. PROFILES

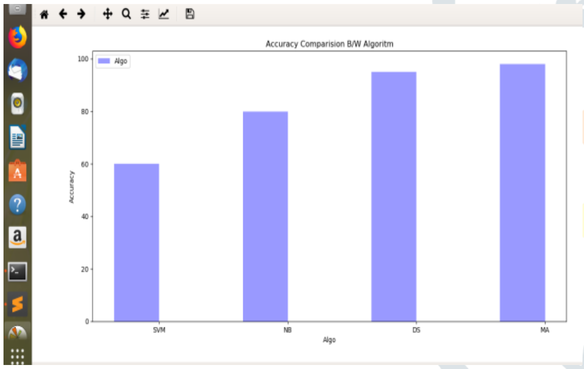
The primary concept behind our strategy is to study the temporal evolution of OSNs and to characterize actual user profiles. If the real-world OSN data can be collected and used to identify a set of statistically consistent features, then these features can be used to study the time evolution of a given test profile and to identify / detect any major deviations from the expected behavior of a profile.[28] Our strategy can thus serve as a first phase identification of prospective false profile, alerting OSN executives to perform further surveillance of the test profile.[29] Based on our data-driven experiments and evaluation, we recognize the following three characteristics that relate to the characteristics of social interaction and social network graphs. Evolution of the amount of OSN buddies over time. • Real social interactions. • Evolution of the OSN chart framework over time. While our concept can be extended to other features of OSN's typical honest social profiles (connection strength, number of tags, number of images, frequency of accepted relationships, and so on), in this article, our goal is to motivate this fresh line of studies with a easy yet effective solution to detect fake profiles. The remainder of this chapter is arranged as follows We first address the method of information collection (Section IV-A). Sections IV-B, IV-D and IV-C therefore demonstrate the function of each of the three parts of our strategy. A. Dataset We developed a Facebook "sensing" application to collect the data we used in this studies that can collect the necessary statistical information from within a profile. The application parses the Facebook wall of a user via Facebook API and gathers data we are interested in. Given a P profile where the application is running, the data gathered concerns the following. • Profile: data on the evolution of the P graph. The application shops for each development of friendship discovered • Friends: Moreover, acting from inside the profile, data retrieved from our application are more detailed even in terms of descriptions. We spread the application by inviting people to run it, starting from a set of people we know. Most of them are 1105 1073 students of our University courses4; others live in our Contains a list of P's friends and all the connections between these friends. Since the application operates from within a profile, it enables us to have a distinct attitude to the remainder of the job in the literature, where high-level studies have been conducted (e.g. interactions are determined by tracking HTTP packets, and social graphs are assessed by observing the static status of a profile and its links). In reality, with our technique, we can have vibrant data, provided that each stream is linked to a timestamp when notified in the user's wall. It's the same town or part of our family. There are also few users we don't understand immediately, but they are friends of friends. Note that the user is informed that the request will send us data and which data will be sent. Indeed, Facebook provides a notification form before installing the application. The form indicates which sort of data the request will be able to obtain from the profile. We are presently collecting information from 80 profiles with our "sensing" implementation, to which we applied the research described in this article. We notice that the information we gathered are not complete for several profiles: That is, we cannot fully reconstruct the user's network chart from the profile development on a day-to-day basis. In reality, this is due to a restriction on the information that Facebook makes accessible even to the profile user: it is not feasible to obtain information in time beyond a particular stage for some profile. Even though, we gathered all possible data to reconstruct the users ' OSN chart evolution for the time interval for which data was accessible.

VII. ADVANTAGE

- It focuses on quantifying, profiling and understanding malicious applications.
- User information is secure and secure.
- Avoid using distinct client IDs in the setup of the app.
- Decrease Fake Account possibilities
- Reduce cybercrime[30]

VIII. RESULT

From the graph we find that the efficiency of the SVM is highest when the data is well trained and the efficiency of the Nave Bayes is lowest, which does not change much when the training dataset t increases. As the amount of features increases the effectiveness of all algorithms for the training dataset. The false positive rate of the SVM is least that means if a profile is recognized as fake then the probability of being fake is very high in SVM whereas Nave Bayes shows a high false positive rate. On the other hand, the false negative rate for Naive Bayes is very low and because the algorithm is well trained, the SVM has an average false negative rate. From the results, we discover that SVM is well suited for the classification of fake profiles in social networks.



IX. Conclusion and future work

We have given a framework through which we can detect fake profiles in an online social network with very high efficiency as high as around 95 percent. Fake profile detection can be improved by using NLP techniques for processing texts and profiles. False identities in the form of compromised or fake email accounts, social media accounts, fake or cracked websites, fake domain names, and malicious Tor nodes are heavily used in APT attacks, especially in their initial phases, and other malicious operations[31-32]. The attacker(s) strive to establish confidence with the goal using these false identities and to craft and mount a spear phishing or other attack. Based on study proof, information gathering for a spear phishing attack depends strongly on the use of social media and false accounts in it. It is therefore essential to identify the existence of a false social media account as soon as possible. A technique based on resemblance of user colleagues was given to detect false accounts in social networks. At first, friend resemblance criteria were calculated from the adjacency matrix of the network graph in this technique and fresh characteristics were extracted from the PCA technique. The information was balanced using the SMOTE in the next phase and sent to the classifier[31].

The classifier was taught and tested using the cross validation method, which showed that the medium Gaussian SVM classifier had an AUC=1

References

[1] Vayansky, Ike & Kumar, Sathish. (2018). Phishing – challenges and solutions. Computer Fraud & Security. 2018. 15-20. 10.1016/S1361-3723(18)30007-1.

[2] Alqatawna, Ja'far & Madain, Alia & Al-Zoubi, Ala & Al-Sayyed, Rizik. (2017). Online Social Networks Security: Threats, Attacks, and Future Directions. 10.1007/978-3-319-55354-2_10.

[3] Jain, Neelesh & Shrivastava, Vibhash & , Professor & Professor, Assistant. (2014). "CYBER CRIME CHANGING EVERYTHING – AN EMPIRICAL STUDY".

[4] AKhonji, Mahmoud & Iraqi, Youssef & Jones, Andy. (2013). Phishing Detection: A Literature Survey. IEEE Communications Surveys &amp Tutorials. PP. 1-31. 10.1109/SURV.2013.032213.00009.

[3] C. C. Wagner, S. Mitter, proprietor of C. K• and M. Strohmaier. Attacking social bots: modeling user susceptibility in online social networks. In WWW Proceedings, volume 12, 2012.

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

[5] A. Wang. Detecting spam bots in social networking locations online: a machine learning strategy. Security and privacy of data and applications XXIV page 335–342, 2010.

[6] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, B.Y. Zhao," Detection and characterization of social spam campaigns" In Proceedings of the 10th Annual Measurement Conference on the Internet, pages 35–47. ACM 2010. ACM 2010.

[7] Z. Z. Chu, S. Gianvecchio, H. Wang, S. Jajodia. "Who tweets on twitter: human"

[8] S. S. Krasser, Y. Tang, J. Gould, D. Alperovitch, P. Judge. Identifying spam picture based on header and file characteristics using c4. 5 Decision trees and vector machine learning aid. Workshop on Information Assurance and Security, 2007. IAW'07. IEEE SMCpages 255-261. IEEE, in 2007.

[9] M. Conti, R. Poovendran and M. Secchiero, "FakeBook: Detecting Fake Profiles in On-Line Social Networks," *2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, Istanbul, 2012, pp. 1071-1078.doi:10.1109/ASONAM.2012.185

[10] V. Tiwari, "Analysis and detection of fake profile over social network," *2017 International Conference on Computing, Communication and Automation (ICCCA)*, Greater Noida, 2017, pp. 175-179. doi:10.1109/CCAA.2017.8229795

[11] J. H. Parmelee and S. L. Bichard, Politics and the twitter revolution: How tweets influence the relationship between political leaders and the public, Lexington books, 2011.

[12]L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: automated identity theft attacks on social networks," in Proceedings of the 18th international conference on World wide web, pp. 551–560, Madrid, Spain, 2009.

[13]L. Jin, H. Takabi, and J. B. Joshi, "Towards active detection of identity clone attacks on online social networks," in Proceedings of the the first ACM conference, p. 27, San

Antonio, TX, USA, Feburary 2011.

[14]M. Conti, R. Poovendran, and M. Secchiero, “FakeBook: Detecting fake profiles in on-line social networks,” in Proceedings of the 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2012, pp. 1071–1078, Turkey, August 2012.

[15]Z. Shan, H. Cao, J. Lv, C. Yan, and A. Liu, “Enhancing and identifying cloning attacks in online social networks,” in Proceedings of the 7th International Conference, pp. 1–6, Kota Kinabalu, Malaysia, January 2013.

[16]G. Kontaxis, I. Polakis, S. Ioannidis, and E. P. Markatos, “Detecting social network profile cloning,” in Proceedings of the 3rd International workshop on security and social networking, USA, 2011.

[17S. Gurajala, J. S. White, B. Hudson, and J. N. Matthews, “Fake Twitter accounts: Profile characteristics obtained using an activity-based pattern detection approach,” in Proceedings of the 2015 International Conference on Social Media & Society (SMSociety'15), Toronto, Ontario, Canada, 2015.

[18]D. Kagan, Y. Elovichi, and M. Fire, “Generic anomalous vertices detection utilizing a link prediction algorithm,” Social Network Analysis and Mining, vol. 8, no. 1, 27 pages, 2018.

[19]Y. Boshmaf, D. Logothetis, G. Siganos et al., “Íntegro: Leveraging victim prediction for robust fake account detection in large scale OSNs,” Computers & Security, vol. 61, pp. 142–168, 2016.

[[20]J. Cao, Q. Fu, Q. Li, and D. Guo, “Discovering suspicious Account in online social networks, Information Science,” Information Science, pp. 1–23, 2017. [21]C. G. Akcora, B. Carminati, and E. Ferrari, “User similarities on social networks,” Social Network Analysis and Mining, vol. 3, no. 3, pp. 475–495, 2013.

[22]J. Santisteban and J. Tejada-Cárcamo, “Unilateral weighted Jaccard coefficient for NLP,” in Proceedings of the 14th Mexican International Conference on Artificial Intelligence (MICAI '15), pp. 14–20, IEEE, Cuernavaca, Mexico, October 2015.

[23]Liyan Dong, Yongli Li, Han Yin, Huang Le, and Mao Rui, “The Algorithm of Link Prediction on Social Network,” Mathematical Problems in Engineering, vol. 2013, pp. 1–7, 2013.

[24]W. Cukierski, B. Hamner, and B. Yang, “Graph-based features for supervised link prediction,” in Proceedings of the International Joint Conference on Neural Network (IJCNN '11), IEEE, San Jose, Calif, USA, 2011.

[25]A. Estabrooks, T. Jo, and N. Japkowicz, “A multiple resampling method for learning from imbalanced data sets,” Computational Intelligence An International Journal, vol. 20, no. 1, pp. 18–36, 2004.

[26]N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, “SMOTE: synthetic minority over-sampling technique,” Journal of Artificial Intelligence Research, vol. 16, pp. 321–357, 2002.

[27]I. Jolliffe, Principal Component Analysis, 2002.

[28]L. Sadowski, M. Nikoo, and M. Nikoo, “Principal Component Analysis combined with a Self Organization Feature Map to determine the pull-off adhesion between concrete layers,” Construction and Building Materials, vol. 78, pp. 386–396, 2015.

[29]V. N. Vapnik, Statistical Learning Theory, Wiley, New York, NY, USA, 1998. [30]S. Sperandei, “Understanding logistic regression analysis,” Biochemia Medica, vol. 24, no. 1, pp. 12–18, 2014.

[31]R. Kohavi, “A study of Cross-Validation and
Bootstrap for Accuracy Estimation and Model
Selection,” in Proceedings of the in 14th