A Walkthrough on Clone Profile Resolution in Social Networks

Liyanage C.R, Premarathne S.C

Abstract— People use Online Social Networks to build social connections with others who are having similar personal interests or coming from the same backgrounds. These social platforms make peoples' life better while generating lots of problems to society. Some attackers perform profile cloning to harvest sensitive data from a targeted person on social media. These attacks will damage the prestige of the legitimate user. Hence to detect such duplicate fake accounts has become a critical necessity of today's online social networks. Many researchers have tried to solve the problem of fake profile detection in online social networks however, more robust solutions are still to be taken. This paper presents a review of approaches in literature for detecting clone profiles.

Index Terms— Classification, Fake profiles, Identity Clone Attack, Online Social Networks, Profile Attributes, Similarity Measures, Social Graph Analysis.

1 Introduction

Online Social Network (OSN) is a web of users connected through user profiles to keep interactions with friends, find news and updates around the world, gain business opportunities, share information and knowledge etc. Due to vast amount of benefits, OSNs have become a significant part of people live where 2.46 billion of the global population is using them and expected to reach around 2.95 billion in 2020 [1]. There are different types of social platforms such as Viber, YouTube, WhatsApp, Facebook, Instagram, Twitter, Google+, LinkedIn etc. and these networks have changed the way of people interact with each other.

Due to socialization nature and extensive usage of OSNs, users tend to expose a vast amount of their personal details to public and these sensitive data can be easily used by malicious users through fake profiles for different purposes [2]. OSN wrongdoers create these fake profiles which do not belong to genuine users either by duplicating an existing user name or by giving non-existing user identity in social media [3],[4]. According to statistical estimations 81million of Facebook accounts and 5 percent of Twitter accounts are fake [5].

In most of the social platforms, user identification is mainly based on limited displayed user details and this makes the user authentication feebler, since it is possible to have more than one account with the same name and many other similar details [6]. Under this capacity Identity Clone Attack (ICA) is one of the most severe security threats in social networks where scammers create identical profiles to existing profiles and appear as someone else in order to steal private information or to damage victims' reputation by publishing inconvenient contents [6],[7],[8]. Hence detection of these clone profiles with fake identities has become one of the crucial tasks in handling social media security and privacy. Researches have introduced various methodologies to verify duplicate profiles in online social networks. This review study investigates approaches that have been introduced to solve the problem of detecting fake clone profiles through single and multiple OSN platforms.

- *Liyanage C.R, Department of IT, Faculty of IT, University of Moratuwa, Sri Lanka. E-mail: ravihari@ictec.ruh.ac.lk*
- *Premarathne S.C, Department of IT, Faculty of IT, University of Moratuwa, Sri Lanka. E-mail: samindap@uom.lk*

2 Review of Literature

Researchers have addressed fake profiles in two aspects either as a duplicate for a specific existing account (profile cloning) or as a new profile with random details. Profile cloning again tested across different platforms which made the security of social network more vigorous. They have selected different social networks and most common selections were Facebook [7], Twitter, Google+ [9] and LinkedIn, where the user profile attributes and behaviors are significantly different.

The study [7] proposes a three-step model to match two different profiles from different social media platforms. They have used a binary classifier for feature extraction based on users' information regarding friend requests and friend lists. This method presents an influential model by using a string-matching similarity algorithm to find profile similarities. However, they have not tested their algorithm using a real dataset. Hence the accuracy and effectiveness of the output is questionable. The authors in [10] have compared the impact of different parameters on verifying the results of the outcomes. First, they have selected the victim and then found list of potential clone profiles. By comparing clones with victims, they have finally verified the results as which profiles are clones.

The study [11] has tried to find clones in social media where the concept was evaluated on users' original profile data to catch similar accounts across OSNs. According to the detected profile similarities, a similarity score has been calculated based on shared values of the information field and profile picture. Another study [9] for detecting duplicate profiles in OSNs has performed and they have considered more similar steps as previous cases [11]. First, they extract information from users' profile such as birthday, age, education, workplace and then extract information from profiles with same names. Finally, they have calculated a similarity index of all the profiles found. Most of the studies have built their ap-

proaches based on attribute similarity models. In paper [12] also have done the same thing but further they have considered about a friend network similarity value.

3 CURRENT STATUS

The area of research for detecting duplicate profiles in online social media networks has evolved recently and most of the research findings were published after 2010. Since the research approaches differ from each other depending on different OSNs, selecting the interest platform is the first most important step. After that finding data sets with interested features, applying suitable methodologies and evaluation of results must be done accordingly. Current background of this research area will be discussed in this section.

3.1 Platform Selection

Single site and cross-site profile cloning are two types of cloning attacks wherein first type creates an account of the victim in the same social network and sends friend requests to victims' friends whereas in cross-site creates an account of victim in a new network and sends requests to friends who are in both networks [6],[13],[9]. According to these two types researchers have developed their fake profile detection algorithms on either specific network or across multiple networks [14]. In present as Facebook is the most popular OSN, many researches have selected it as the platform for their research work [3],[15],[16]. Not only that, some authors have used multiple platforms such as Google+ and Twitter along with the Facebook as their social environments [4],[17].

3.2 Data Collection

In each profile in OSN provides lots of qualitative and quantitative information such as gender, location, education, work, age, number of friends, comments, likes. However, this information provides different accessibilities for different audiences since some are public and others are private [3]. In many researches public data has been used due to limitations of gathering private data of profiles [14],[18]. However, in [7] the author has not used a real data set for his implementation. Data gathering has mainly carried out in several ways where creating experimental fake profiles or called as "Honey profiles" has done by [16] and this method was better than the way of data gathering via APIs, since researchers can gain data by controlling the conditions as they want. They have created several honey profiles with different features and collected data once each day for one month. However, this method has limitations when considering vast amount of data collections.

Some researchers have collected real profile information using Facebook Graph API along with Python [4],[3] and fake profile dataset has provided by Barracuda Labs [3]. Some data has scrapped from friend accounts and for that they have implemented an anti-scrap detection technique to prevent Facebook from detecting [3]. Paper [4] has used a fixed number of profiles around 3000 and these were downloaded from Stanford Network Analysis Platform (SNAP Library). They have divided the dataset into two parts one half as real profiles and other as fake profiles. Another study [15] has collected their initial data set of 4.4million public posts using post search API of Facebook. Social Snapshot tool developed by Huber is one of the tools used in [16] to collect Facebook user data.

3.3 Approaches

3.3.1 Using Classification Algorithms

Some algorithms have tried to solve this problem of identifying OSN fake profiles based on classification approaches. In [3] the author has used three classification algorithms, Support Vector Machine (SVM), Naive Bayes and Decision trees and have compared the efficiency among each. After selecting the profile to be tested they have extracted the required features (Gender, Number of friends, education and work, relationship status, numbers of photos tagged, number of uploaded photos etc.) and then using the classifier determined whether the profile is fake or not. Then again, the result has used to train the classifier in order to obtain more accurate predictions. According to the results SVM has selected as the best classification model where Naïve Bayes has given the lowest performance. Another research study [15] has conducted to find malicious Facebook pages using Artificial Neural Networks. The set of words in published contents has used to differentiate malicious and true pages.

Some approaches were there to find user profiles belong to the same user over different social networks [18]. They have generated a similarity vector using a known dataset of paired accounts belongs to the same user across multiple networks. Then these vectors were used as the training dataset for supervised classifiers such as KNN, Naïve Bayes, Decision trees and SVM. However, this approach is using more static attributes (Name, Location, Description, Profile image and Number of connections) when considering similarity vector whereas in some approaches use more dynamic behavioral features like in [17] which have shown more robust and accurate results.

3.3.2 Social Grapgh based Approach

In paper [4] the author introduces a detection mechanism called Fake Profiles Recognizer (FPR) which authenticate and recognize his trusted friends as well as detect fake ones by modeling the online social network graph after representing the identity of each user as a Friend Pattern. A profile will be a fake to a selected profile, if it has indicated by a fake instance which came from another friend pattern and will not accepted by the friend pattern processor. This friend pattern has used to distinguish duplicate profiles in OSN. This approach has proved higher accuracy than SVM [3] and lower F-Measure values than Naïve Bayes approaches [3]. However, in case of lesser number of fake profiles this algorithm has unable to recognize the fake profiles. A case study [16] has performed by illustrating its friendship network using graphs where nodes represented profiles and friendships among profiles represented edges. They have presented some concepts such as network density, degree of nodes, and the correlation between nodes in the process of identification fake nodes. Finally, they have concluded that the profiles with lesser number of activities and high number of friends have more chance to be fakes.

The approach [13] has evaluated the identity of clone profiles in the same network using two concepts in which the second one is based on its' strength of the relationship measures. For this, social network data were modeled using a weighted

graph and they have tried to consider user interactions not only based on friend requests, rather considered more linkage between profiles such as active friends, page likes, URLs, friendship graph and mutual friends' graph.

In [19] a novel social graph topology called "Trusted Social Graph (TSG)" has introduced by using a special type of graph called "DeBruijn graph" to visualize the trusted instances within the social network. They have analyzed the social profiles by evaluating their friend patterns using mathematical expressions. Finally, the incoming instances were checked against the model and decided whether that profile is fake or real.

Some algorithms like [20] have presented a method to detect clone profiles using a graph and network-based approach by analyzing the structural similarity of the social network. The
authors have first selected a node to analyze from an analyzed network and get the nearest neighbors considered node. After measuring the similarity of nodes, it will detect duplicate profiles as gave highest frequency of attribute similarities. Furthermore, due to the usage of k-nearest neighbor algorithm, this approach was able to recover hidden values of attributes of user profiles.

3.3.3 Matching Similarity Attributes

In study [14] the similarity of two profiles has been checked based on their HTML structures. They have conducted techniques on exact matching of attributes to match usernames by doing string comparisons and partial matching of related attributes to match parts of profile attributes such as location and address. The paper [7] has also used a similarity matching algorithm but it has shown higher results due to its recursive matching technique. As mentioned under graph-based approach, the study [13] has evaluated the profile identity using two concepts which the first one was based on calculating profile similarity using selected attributes, the first name, family name and location. After filtering suspicious accounts based on these attribute similarities, they are evaluating the strength of relations and finally have identified the fakes. The literature has introduced another approach [10] to detect profile clones by comparing five different similarity measures which includes two more additional attributes, gender and education details than given in study [13]. However, this study has used a limited dataset for their developments.

The methods like [9] have calculated a similarity index after comparing the original profile and other searched accounts. They have assumed if the similarity index is high the profiles may be cloned. However, the other assumption they have made as the fake profiles will give the lowest similarities is not acceptable since there can be profiles with less similarities to each other but still real. The approach [12] has introduced a weighted dice similarity measurement to calculate the similarity of selected attributes. They have assigned weights according to the importance of each attribute for each person. This method can give more reliable results since the importance of attributes may vary from person to person. Some algorithms [11] have directly matched the strings in information fields to measure the similarities between profiles. However, in case of incorrectly typed information this method will give inaccurate results. Same as most of the approaches, the paper [21] has also discussed about an attribute similarity and friend network similarity approach. They have considered three types of friend network features for analysis, friend list, recommended friend list and excluded friend list. Furthermore, the study [16] has focused more on analyzing the location-based attributes such as work and educational places and current locations and has found that these will give stronger factors in fake identifications. In paper [22], researchers have used 17 profile features to evaluate the similarities between profiles and this is a very high number comparing to other existing researches. Not only that, they have used 12 classifiers for the task of detecting fake profiles.

3.3.4 Analyzing User Behavior Changes

According to [6] the interested features can be categorized into two as behavioral and non-behavioral attributes. Due to the anomalous behavior of fake profiles they are easy to identify by analyzing behavioral patterns [17]. Paper [15] has used a bag-of-words collected from recent activities of Facebook pages and extracted patterns from them. Also, they have analyzed the behavior changes in such pages. The approach [17] has used a combination of statistical models and sudden behavioral changes in user profiles to detect fakes. They have considered detecting only the malicious behavioral changes for their algorithms since users can experience sudden changes in their behaviors due to many other legal reasons as well. In [23] the authors have used a text mining approach to measure the similarity between text information such as posts and comments on two types of social media public pages.

3.3.5 Matching User Profiles Across Multiple OSNs

Since people tend to use different social network platforms many researches have focused on detecting fake profiles across different types of platforms [7]. This kind of detection is more difficult than single site detection due to necessity of analyzing different networks and different features of those profiles [21].

4 DISCUSSION

Among most of the security issues in online social networks, fake profile identification gained more importance since it can lead to severe security and user privacy threats. Identity Clone Attack is one of the fake profile problems which was considered as the most dangerous threat in OSN. Hence, the detection of clone profiles has become an important area in the research field of computer science all over the world and 75 percent of the existing solutions were found after 2010.

The detection of clone profiles in social networks is a currently engaging research problem and most of the investigations are done using Facebook, as it is the most popular social network platform. Other than that Twitter is also a widely used network since there are less privacy concerns when creating user profiles. When considering the selected platforms of past researches, the networks having less complex process for creating user profiles and weak user authentication mechanisms have mostly been subjected to the fake profile issue.

Some researchers [7] have used synthetic data sets for their

investigations and these may not give the most realistic solutions since social networks are highly diverse environments and this complex diversity can be efficiently gain only using real data. However, still most of the researches made their assumptions using very limited amount of real data since it is difficult to get personal user data through an API due to confined accessibilities.

There were different methodologies for detecting clone profiles in OSNs, but the most common type was to match the profiles using similarity measurements where study [22] has used large number of attributes for this consideration. Moreover, graph-based approaches have been used to analyze friend networks in OSNs to consider the compactness and strength of networks to predict clone profiles. Classification in data mining was another common technique to analyze user data in the platforms and Decision Trees and Naïve Bayes were the most used ones.

However, due to the diverse characteristics and rapidly changing nature of social networks, fake clone profile detection is still not fully solved by existing approaches and opened for future directions

5 FUTURE DIRECTIONS

Some proposed techniques have been found after investigating current approaches. The study [14] has suggested a biometric authentication method to use user fingerprints, voice and signatures to verify the identity of a user in a social network platform. This may result more accurate solutions since biometric characters are unique to each person. Some [20] have proposed a user relationship prediction model to forecast future clone profiles. This will be more useful since prevention of attack is better than detection after the attack.

6 CONCLUSION

Identity Clone Attack is a severe threat in Online Social Networks which was spread over the recent years and it cause damages to the legitimate users in the network due to misusing the personal information. Several researches have taken attempts to solve this problem by detecting clone profiles in different social platforms and their experimental techniques are mostly based on statistical estimations, data mining techniques and behavioral analysis methodologies etc. However, due to the difficulty of finding real datasets for researches and the higher diversity of profiles in these networks, a fully compatible solutions are still to be taken.

REFERENCES

[1] Statista, "Social Media Statistics & Facts," 2017. [Online]. Available: https://www.statista.com/topics/1164/social-networks/. [Accessed: 30-Oct-2017].

[2] M. Fire, D. Kagan, A. Elishar, and Y. Elovici, "Social Privacy Protector - Protecting Users ' Privacy in Social Networks," no. c, pp. 46–50, 2012.

[3] N. Kumar and R. N. Reddy, "Automatic Detection of Fake Profiles in Online Social Networks," National Institute of Technology Rourkela Rourkela-769 008, Orissa, India, 2012.

[4] M. Torky, A. Meligy, and H. Ibrahim, "Recognizing Fake Identities in Online social Networks based on a Finite Automaton Approach," 2016 12th Int. Comput. Eng. Conf. ICENCO 2016 Boundless Smart Soc., pp. 1–7, 2017.

[5] WordStream, "40 Essential Social Media Marketing Statistics for 2017," 2017. [Online]. Available: http://www.wordstream.com/blog/ws/2017/01/05/social-media-marketing-statistics. [Accessed: 10-Nov-2017].

[6] M. A. Wani and S. Jabin, "A Sneak into the Devil's Colony - Fake Profiles in Online Social Networks," 2017.

[7] G. A. Kamhoua et al., "Preventing Colluding Identity Clone Attacks in Online Social Networks," in 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), 2017, pp. 187–192.

[8] M. Fire, R. Goldschmidt, and Y. Elovici, "Online Social Networks: Threats and Solutions Survey," IEEE Commun. Surv. TUTORIALS Online, vol. 16, no. 4, pp. 1–20, 2013.

[9] M. A. Devmane and N. K. Rana, "Detection and Prevention of Profile Cloning in Online Social Networks," Int. Conf. Recent Adv. Innov. Eng. ICRAIE 2014, pp. 9–13, 2014.

[10] P. Bródka, M. Sobas, and H. Johnson, "Profile Cloning Detection in Social Networks," Proc. - 2014 Eur. Netw. Intell. Conf. ENIC 2014, pp. 63–68, 2014.

[11] G. Kontaxis, I. Polakis, S. Ioannidis, and E. P. Markatos, "Detecting Social Network Profile Cloning," 2011 IEEE Int. Conf. Pervasive Comput. Commun. Work. PERCOM Work. 2011, pp. 295–300, 2011.

[12] M. R. Khayyambashi and F. S. Rizi, "An Approach for Detecting Profile Cloning in Online Social Networks," 2013 7th Intenational Conf. e-Commerce Dev. Ctries. With Focus e-Security, ECDC 2013, pp. 1–12, 2013.

[13] F. Rizi, M. Khayyambashi, and M. Kharaji, "A New Approach for Finding Cloned Profiles in Online Social Networks," Int. J. Netw. Secur., vol. 6, no. April, pp. 25–37, 2014.

[14] B. B. Das, "Profile Similarity Technique for Detection of Duplicate Profiles in Online Social Network," vol. 7, no. 2, pp. 507–512, 2016.

[15] P. Dewan, S. Bagroy, and P. Kumaraguru, "Hiding in Plain Sight : Characterizing and Detecting Malicious Facebook Pages," pp. 193–196, 2016.

[16] K. Krombholz, D. Merkl, and E. Weippl, "Fake Identities in Social Media: A Case Study on the Sustainability of the Facebook Business Model," J. Serv. Sci. Res., vol. 4, no. 2, pp. 175–212, 2012.

[17] M. Egele, C. Kruegel, and G. Vigna, "COMPA : Detecting Compromised Accounts on Social Networks."

[18] A. Malhotra, L. Totti, W. Meira, P. Kumaraguru, and V. Almeida, "Studying User Footprints in Different Online Social Networks," Proc. 2012 IEEE/ACM Int. Conf. Adv. Soc. Networks Anal. Mining, ASONAM 2012, pp. 1065–1070, 2013.

[19] A. M. Meligy, "A Framework for Detecting Cloning Attacks in OSN Based on a Novel Social Graph Topology," no. February, pp. 13–20, 2015.

[20] M. Zabielski, R. Kasprzyk, Z. Tarapata, and K. Szkółka, "Methods of Profile Cloning Detection in Online Social Networks," MATEC Web Conf., vol. 76, 2016.

[21] F. S. Rizi and M. R. Khayyambashi, "Profile Cloning in Online Social Networks," Int. J. Comput. Sci. Inf. Secur., vol. 11, no. 8, pp. 82–86, 2013.

[22] A. Gupta and R. Kaushal, "Towards Detecting Fake User Accounts in Facebook," ISEA Asia Secur. Priv. Conf. 2017, ISEASP 2017, vol. 1, pp. 1–6, 2017.

[23] H. Agrawal and R. Kaushal, "Analysis of Text Mining Techniques over Public Pages of Facebook," in Proceedings - 6th International Advanced Computing Conference, IACC 2016, 2016, pp. 9–14.