THE IMPACT AND MANAGEMENT OF ONLINE SOCIAL NETWORKS: DETECTION OF FAKE AND CLONE PROFILES

Ravinder Kumar
M.Tech Computer Science, UIET MDU, Rohtak, Haryana

Cite This Article: Ravinder Kumar, "The Impact and Management of Online Social Networks: Detection of Fake and Clone Profiles", International Journal of Current Research and Modern Education, Volume 4, Issue 2, Page Number 19-22, 2019.

Abstract:

The proliferation of Online Social Networks (OSNs) has significantly altered communication patterns, facilitating unprecedented levels of interaction, content sharing, and collaboration across the globe. These platforms, including Facebook, Twitter, LinkedIn, and Research Gate, play pivotal roles in both social and professional domains. However, the rise of OSNs has also introduced complex challenges, particularly in terms of security and trustworthiness, such as the prevalence of fake and clone profiles. This study explores the architecture of OSNs, their influence on various sectors including marketing, sociology, and politics, and delves into the critical issues arising from the misuse of these platforms, including privacy concerns and the spread of misinformation. We further analyze methods for detecting fake and clone profiles, focusing on attributes and network similarity measures like cosine similarity and Levenshtein distance. Through data visualization, we present an overview of the distribution of fake versus real accounts, highlighting the ongoing struggle against fraudulent activities within OSNs. Our findings underscore the need for advanced detection techniques and robust security measures to safeguard users and enhance the integrity of online social networks.

Key Words: Online Social Networks, Fake Profiles, Clone Profiles, Data Visualization, Network Similarity, Attribute Similarity, Social Media Security.

Introduction:

A collection of nodes (people, actors, organizations, countries, and states, etc.) connected by a network of links (relationships, interactions, distances, hyperlinks, etc.) is known as an online social network (OSN). Web applications that are primarily used on OSNs are developed to encourage user involvement, teamwork, and content sharing. OSNs have altered how people think, communicate, and interact with others. Several social networking websites, including Facebook, Twitter, Flickr, People utilize websites like LinkedIn, Research Gate, and others to conduct their social and professional endeavours. OSNs' structure is similar to that of real-world systems, therefore Communities are quite valuable since they contain a ton of user content significant to academics and experts in a number of other fields, such as marketing, sociology, government, etc. To develop tactics for viral marketing, marketing firms research OSNs. Sociologists utilize them to study human behaviour and help businesses reach their potential customers.

The collections of nodes (people, actors, organizations, countries, and states, etc.) that make up an online social network (OSN) are joined by a network of links (relationships, interactions, distances, hyperlinks, etc.). Web applications that are predominantly OSNs are referred to as aimed for promoting user connection, teamwork, and content sharing. Onstage altered how people communicate, think, and interact with the outside world. There are numerous social networking services available now, including Facebook, Twitter, Flickr, People use websites like LinkedIn, Research Gate, and others for social and professional pursuits Given that OSNs' structure resembles that of real-world systems, Communities are highly valued since they contain a significant volume of user content vital to the academics and a number of other academic fields like marketing, sociology, etc., politics To create viral marketing techniques, marketing firms research OSNs. Sociologists use them to examine how businesses may attract new clients and Politicians make use of them to strengthen their electoral campaigns. There is a huge diversity of OSNs based on the traits. Social networks, for instance, assist users in creating online social ties with friends and family. These OSNs include Twitter, Facebook, Myspace, and others.

The most popular social network on the internet, Facebook gives members a place to connect and share information with those they know. Twitter allows users to share their ideas, viewpoints, and proposals while also getting updates from other users who are connected to them. Some social networking sites, like YouTube and Flickr, are made particularly to offer a simple and handy way to exchange movies and photographs. There are also online networking tools like LinkedIn that are primarily created to foster users' professional development. It is an online professional network that gives users a potent way to interact with others doing the same type of work.

Fake Profile Detection:

We can check fake profiles by keeping a check of profiles with no profile image or profile name. This method is used to detect all fake Twitter profiles. Here, fake profiles detection is based on rules that can differentiate fake profiles from genuine or real ones. The geo-enabled field feature will come out as false since they do not want to expose their personal location in any tweets. Fake profiles either make a lot of tweets or don't make any tweets. The rules gets applied on the profile initially and, for each matching rule, a counter gets incremented, often it happens that the counter value comes out to be greater than predefined threshold, and in that case, the profile is termed as fake account.

Clone Profile Detection:

In this module, detection clones are based on Attributes and Network similarity. We can take user profiles as input. This module follows a search mechanism in which profiles having attributes matching to that of the user's profile are looked. it calculates similarity index based on the columns obtained and if the similarity index comes out greater than the threshold, then the profile can be stated as clone, else considered normal.

- Attribute Similarity: Attribute similarity is analysed on the basis of similarity of attribute data or values obtained between the profiles. The attributes which are taken into consideration for similarity measures are Name, Profile Name, Language, Location and Time zone, Contact details, E-mail ids, etc. Two major similarity measures are being followed to find the similarity between the attributes or columns. These two measures include Cosine similarity and Lowenstein distance. The Cosine similarity is used to find similarity between the words. The next measure, that is Lowenstein distance, is applied to find similarity between two sequences. The cosine similarity measure is given by; two different vectors can have a cosine similarity of 1 if they have the same orientation. Similarly; two vectors will have a similarity of 0 if they are fixed at 90° and -1 if they are diametrically opposed. The Lowenstein distance method is a similarity measuring system to find similarity among two sequences. If we are provided with two sequences, the Lowenstein distance between them will be the minimum number of inserts, substitution or delete operations needed to convert one sequence into another.
- Network Similarity: Network similarity is analysed on the basis of network relationships. Here, network attributes are used such as Follower's id's attribute have been in play to find the network similarity between different profiles. Attribute Follower's id's keeps a record of the list of accounts that follows the concerned user. All clone profiles that exist try to keep their profiles as much similar as possible to the legit original account.

Findings:

Detection of such fake profiles is a very challenging task among the huge source of web, data and links available. The major issues that are arising due to social media networks can be examined in following points:-

- People should not reveal their true identity on social media platforms according to privacy policies. The authenticity of true identity has been questioned very often and this affects the people who are falsely accused or been misled by resources.
- The ease with which fake accounts and malicious activities are happening around is among the major issues. False accounts being bought at online marketplace at minimal costs. It has been so easy to buy fake followers and like for social sites like Instagram, Face book and Twitter, etc.
- The miss-authentication of social media sites by having more followers, likes and comments leads to gaining more attention and social popularity. This trend motivates individuals to seek out new artificial or manual means to keep ahead of the competition.
- It is well-known that social media platforms are susceptible to a new term known as a Sybil attack, in which an attacker or fraud maintains a large number of phony accounts and utilizes them to conduct a variety of hostile acts.
- Groups which are especially made to spread chaos and miss-conception on social issues or for spamming activities. Fake news circulated across social media about Hurricane Sandy in the US. The news became viral in such a short time in spite of being fake and became a major source of information for those who got affected by the storm.

According to current scenario and graph analysis, most of the audience uses manual methods to detect fake accounts. A fake account doesn't use genuine words; it gets more involved into persuasive words. Fake accounts can be identified by analysing the algorithm and actions followed by any account. Bogus up-sides can possibly truly disable clients' encounters, consequently quick move ought to be made to suspend accounts that are believed to be deceitful. Social media networks haven't totally mechanized the most common way of removing false records.

Performing Data Visualization:

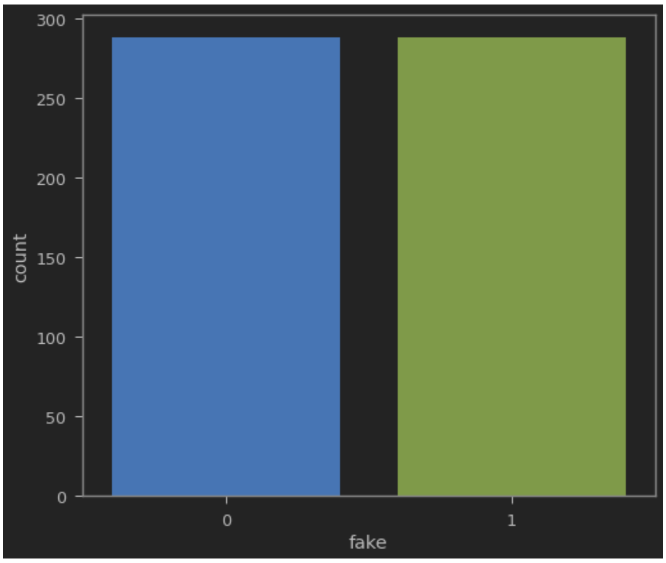

Figure1: Visualizing the number of fake and real accounts (own source)

In the presented graph, each data point represents a profile, and the graph visualizes whether each profile is categorized as "trusted" (0) or "fake" (1). The horizontal axis likely represents individual profiles, while the vertical axis indicates the classification label assigned to each profile. By analyzing the distribution of data points along the vertical axis, one can determine the proportion of profiles categorized as trusted (0) versus fake (1). This visualization offers a quick and intuitive way to understand the distribution of fake and real profiles within the dataset.

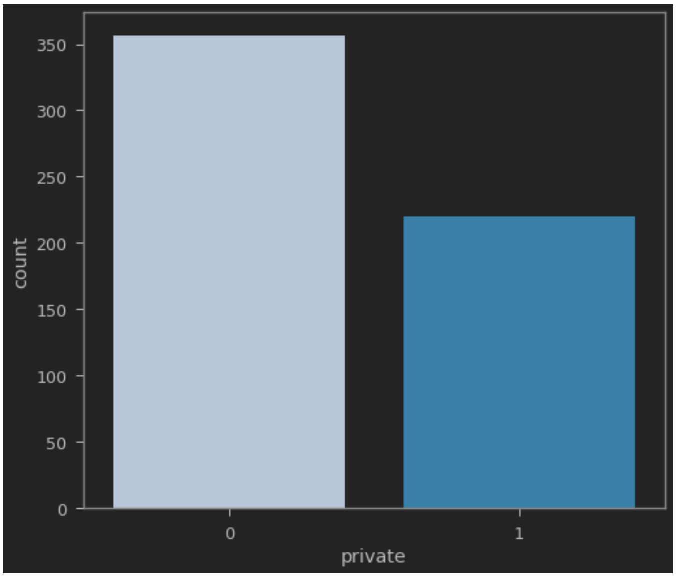

Figure 2: Visualizing the private column (own source)

The graph here represents the privacy of profile, number of profiles has made their setting on private profiles It can be drawn that over 350 profiles are trusted profiles and 200 are fake who have made their profiles private.

Conclusion:

The dynamic landscape of Online Social Networks (OSNs) has transformed human interaction, collaboration, and information sharing, serving as a cornerstone for both personal and professional engagement. With their resemblance to real-world systems, OSNs offer vast repositories of user-generated content, providing invaluable insights into human behavior, marketing strategies, and political campaigns. However, alongside their benefits, OSNs harbor significant challenges, including the emergence of fake and clone profiles that jeopardize user security and the authenticity of online interactions. Our study highlights the complexity of detecting such fraudulent activities, emphasizing the importance of leveraging attribute and network similarity metrics for effective identification. The visual representation of fake versus real accounts further illuminates the extent of this issue, underlining the necessity for continuous improvement in detection methodologies. Addressing these challenges is crucial for maintaining the integrity of OSNs and protecting users from the potential harms of digital deception. As OSNs continue to evolve, ongoing research and development of sophisticated security measures will be paramount in ensuring a safe and trustworthy online environment for all users.

References:

1. Hao, P. and Wang, X., 2019. Integrating PHY security into NDN-IoT networks by exploiting MEC: Authentication efficiency, robustness, and accuracy enhancement. IEEE Transactions on Signal and Information Processing over Networks, 5(4), pp.792-806.
2. Fire, M., Goldschmidt, R. and Elovici, Y., 2014. Online social networks: threats and solutions. IEEE Communications Surveys & Tutorials, 16(4), pp.2019-2036.
3. Al-Qurishi, M., Rahman, S.M.M., Hossain, M.S., Almogren, A., Alrubaian, M., Alamri, A., Al-Rakhami, M. and Gupta, B.B., 2018. An efficient key agreement protocol for Sybil-precaution in online social networks. Future Generation Computer Systems, 84, pp.139-148.
4. Foody, M., Samara, M. and Carlbring, P., 2015. A review of cyber bullying and suggestions for online psychological therapy. Internet Interventions, 2(3), pp.235-242.
5. Sapountzi, A. and Psannis, K.E., 2018. Social networking data analysis tools & challenges. Future Generation Computer Systems, 86, pp.893-913.
6. Zhang, Z. and Gupta, B.B., 2018. Social media security and trustworthiness: overview and new direction. Future Generation Computer Systems, 86, pp.914-925.