Detection of Fake and Clone Accounts in Twitter

[1]L. Kanya kumari, [2]Shaik Nagur Meeravali, [3]Jijjuvarapu Rajesh, [4]Yarlagadda Dhanush Pani, [5]Gumma Subbayya

[1]Assistant Professor Department of Information Technology, Andhra Loyola Institute of Engineering and Technology, Vijayawada,AP, INDIA
[2,3,4,5]UG Students, Department of Information Technology, Andhra Loyola Institute of Engineering and Technology, Vijayawada,AP, INDIA

Abstract: Online Social Network (OSN) is a network hub where people with similar interests or real world relationships interact. As the popularity of OSN is increasing, the security and privacy issues related to it are also rising. Fake and Clone profiles are creating dangerous security problems to social network users. Cloning of user profiles is one serious threat, where already existing user's details are stolen to create duplicate profiles and then it is misused for damaging the identity of original profile owner. They can even launch threats like phishing, stalking, spamming etc. Fake profile is the creation of profile in the name of a person or a company which does not really exist in social media, to carry out malicious activities. In this paper, a detection method has been proposed which can detect Fake and Clone profiles in Twitter. Fake profiles are detected based on set of rules that can effectively classify fake and genuine profiles. For Profile Cloning detection two methods are used. One using Similarity Measures and the other using C4.5 decision tree algorithm. In Similarity Measures, two types of similarities are considered – Similarity of Attributes and Similarity of Network relationships. C4.5 detects clones by building decision tree by taking information gain into consideration. A comparison is made to check how well these two methods help in detecting clone profiles.

Check for updates

DOI of the Article: https://doi.org/10.46501/IJMTST0707054

Available online at: http://www.ijmtst.com/vol7issue07.html

As per UGC guidelines an electronic bar code is provided to seure your paper

To Cite this Article: L. Kanya kumari; Shaik Nagur Meeravali; Jijjuvarapu Rajesh; Yarlagadda Dhanush Pani and Gumma Subbayya. Detection of Fake and Clone Accounts in Twitter. *International Journal for Modern Trends in Science and Technology* 2021, *7*, 0707131, pp. 319-323. https://doi.org/10.46501/IJMTST0707054

Article Info. Received: 14 June 2021; Accepted: 12 July 2021; Published: 26 July 2021

I. INTRODUCTION

Billions of users use online social networks (OSN) like facebook, twitter, linkedin, instagram, and others to create network connections. The comfort and convenience the ubiquity of social media has ushered in a new era of creativity. Networking. in the OSN, users share a lot of information.images, videos, the name of the school, the name of the college, and so on contact information, such as phone numbers, email addresses, and home addresses, as well as family ties, details about your bank account, your job, and so on. If this information is put into practise, the consequences of the assailants' actions are devastating. The majority of users of OSN are unaware of the security risks that exist in social media and are thus vulnerable to these assaults. The if the victims are minors, the dangers are multiplied. In the spotlight existing users' profile information is cloned in a cloning attack. Stolen in order to build duplicate profiles, which are then used to spread malware. Abused to reveal the identities of the original profile owners [1-6]. There are two forms of profile cloning: same-site cloning and off-site cloning. Cloning of cross-site profiles [1,7-9].

If user credentials from one network are used to create a new network, when you clone a profile in the same network, it's referred to as same site. Cloning of profiles [1,10-12]. In cross-site profile cloning, the attacker copies a user's profile from one site to another. Takes the user data from one network and creates a new one duplicate profile in another network that the user is not a member of having an account of any kind [1, 13-15].

As the registration process for social media sites has become more complicated, easy in order to attract a growing number of users, fake profiles are likewise being created at an alarming rate. In order to connect to a target, an attacker generates a phoney profile. To be used as a scapegoat for evil activities also, to disseminate bogus news and unsolicited messages the following is a breakdown of the paper's structure. The second section discusses the review of the literature the proposed solution is explained in section III methodology. The results are discussed in section IV. Finally, section with the conclusion, V brings the paper to a close.

II. LITERATURE SURVEY

Fake and clone profiles have become a major problem in social media today. As a result, a strategy for detecting these fraudsters who utilise people's faith to obtain private information and generate duplicate profiles is critical. Many academics have contributed to this field and proposed ways for detecting these types of profiles in social media. Some of these techniques are detailed further down.

Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis, and Evangelos P Markatos [2] suggested a prototype for determining whether or not users have been cloned.Information is collected from the user profile, and a search in OSN is performed to locate profiles that match the user profile, with a similarity score determined based on attribute value similarity. When the similarity score exceeds a certain level, the profile is considered cloned.

Brodka, Mateusz Sobas, and Henric Johnson proposed two unique approaches for recognising cloned profiles in their study [3]. The first method is based on attribute value similarity between original and cloned profiles, while the second method is based on network relationships. A victim will be chosen from those who believe their profile has been copied. Then, using query search, a search for profiles with the same name as the victim is conducted, using name as the primary key. The Victim profile (Pv) and the Potential clone (Pc) are compared, and the similarity S is computed. If S(Pc, Pv) is more than Threshold, the profile is likely to be a clone. The user performs the verification stage manually since he knows which profile is his original and which is a replica.

In their study, Cresci S, Di Pietro R, Petrocchi M, Spognardi A, and Tesconi M [4] analyse some of the most relevant existing features and rules (presented by Academia and Media) for detecting fraudulent Twitter accounts. They trained a collection of machine learning classifiers using these rules and features. Then they developed the Class A classifier, which can distinguish between genuine and bogus accounts.

A classification approach for detecting bogus accounts on Twitter has been proposed by Ahmed El Azab, Amira M Idrees, Mahmoud A Mahmoud, and Hesham Hefny [5]. They gathered several useful features for the identification process from various studies and filtered and weighted them in the first stage.

Various studies are carried out in order to find the smallest collection of features that produce accurate results. Only seven attributes were chosen among 22 to efficiently detect bogus accounts, and these factors were applied to classification systems. The classification techniques are compared based on the results, and the one that offers the most accurate result is chosen.

III. PROPOSED SYSTEM

Fake and clone profiles have become a major social issue. Because information such as phone numbers, email addresses, school or college names, corporate names, and locations are publicly available on social media sites, hackers can easily use this data to construct bogus or clone identities. They then attempt to perpetrate various attacks such as phishing, spamming, cyberbullying, and so on. They even go so far as to try to discredit the legitimate owner or organisation. So, in order to make users' social lives more secure, a detection approach has been presented that can detect both fake and clone profiles. The suggested system's architecture is depicted in Figure 1.

The proposed architecture consists of modules for Fake Profile detection and Clone Profile detection.

A. Fake Profile Detection

This module is used to identify bogus Twitter accounts. False profiles are recognized using methods that efficiently differentiate fake profiles from authentic profiles. Some of the rules are as follows: that are utilized to detect bogus profiles include - false profiles are usually There is no profile name or photograph. They are devoid of any. Description of the user account the field will be geo-enabled. They don't want their location to be revealed in tweets, so this is incorrect.

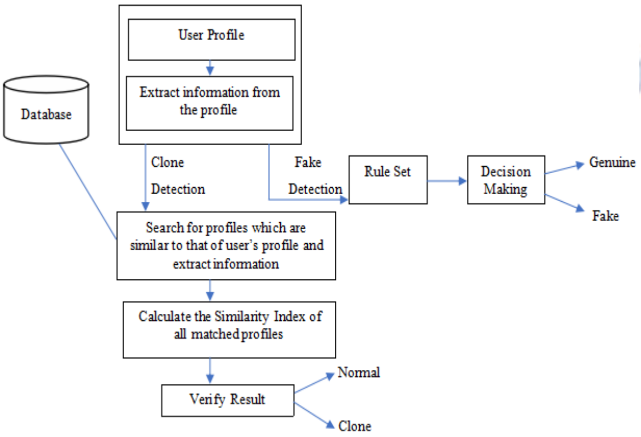
User Profile
Extract information from the profile
Database
Clone Detection
Fake Detection
Rule Set
Decision Making
Genuine
Fake
Search for profiles which are similar to that of user's profile and extract information
Calculate the Similarity Index of all matched profiles
Verify Result
Normal
Clone

Fig. 1. Architecture of proposed system.

They usually send out a high number of tweets, or the profiles may not have sent out any at all. The rules are applied to the profile, and a counter is incremented for each matching rule; if the counter value exceeds a pre-defined threshold, the profile is considered phoney.

B. Clone Profile Detection using Similarity Measures

Based on Attribute and Network similarities, this module discovers clones. As input, the user profile is used. The profile contains information that can be used to identify the user. Profiles with attributes that match the attributes of the user's profile are searched. The similarity index is calculated, and if it exceeds the threshold, the profile is classified as clone, otherwise as normal[1].

i) Attribute Similarity

The similarity of attribute values between the profiles is used to determine attribute similarity. Name, ScreenName, Language, Location, and Time zone are the attributes that are taken into account while measuring similarity. The similarity between the qualities is measured using two similarity measures: Cosine similarity and Levenshtein distance.Similarity between words is determined by cosine similarity, and similarity between two sequences is determined by Levenshtein distance.

Equation gives the cosine similarity formula (1)

$$\cos(\theta) = \frac{\sum_{i=1}^{n} A_i B_i}{\sum_{i=1}^{n} A_i^2 \sum_{i=1}^{n} B_i^2} \quad (1)$$

where A_i and B_i are two non-zero vectors [1].

If two vectors have the same orientation, they have a cosine similarity of 1; if they are at 90°, they have a similarity of 0; and if they are diametrically opposing, they have a similarity of -1 [1]. The Levenshtein distance is a similarity metric for determining how similar two sequences are.

ii) Network Similarity

On the basis of network relationships, network similarity is calculated [1]. The Followers ids attribute is used to compare the profiles' network similarities. The list of accounts that follow the user is given by followers ids. To prove that it is real, the clone profile tries to connect to the same group of users as the legitimate owner. We may determine whether two profiles are similar in terms of network linkages by comparing their Followers ids.

C. Clone Profile Detection using C4.5 algorithm

The C4.5 method is used in this module to determine whether a given profile is a clone or not. C4.5 is a classification algorithm based on a decision tree. It creates a decision tree depending on the information provided. The property that most effectively divides the sample sets into subgroups is chosen at each node of the tree.

Information gain and entropy are the splitting factors utilised in C4.5. To make a decision, the attribute with the maximum information gain is picked, and it then recurses through the partitioned sub-trees. As illustrated in equation, the knowledge gain (2)

$$\text{Info(D)=-}\sum(i=1)^{n}\left[P_i \log 2P_i\right] \quad (2)$$

By constructing a tree-like structure, the C4.5 method determines the degree of similarity between the qualities. The given profile is compared to profiles previously stored in the database. If the given profile matches one of the profiles in the database, it is considered a clone; otherwise, it is considered normal.

IV. EXPERIMENTS AND RESULTS

A. Datasets Used

The experiment's datasets were gathered from MIB initiatives. It's made up of both real and fake Twitter datasets. The Genuine accounts dataset is made up of accounts from scholars, social specialists, and journalists from Italy, the United States, and other European nations who volunteered to be part of an academic study on detecting fraudulent accounts on Twitter. Fastfollowerz.com, intertwitter.com, and twittertechnology.com [4] are three separate Twitter online markets where the phoney accounts were purchased.

B. Evaluation Metrics

Various evaluation metrics based on the following four standard indications are used to evaluate the system's performance.

- True Positive (TP): True positives are records that are recognised accurately using expected vectors.
- True Negative (TN): True negatives are records that were correctly identified as Neutral but were not.
- False Positive (FP): False positives are records that were expectedly detected by the system but are instead listed in different vectors.
- False Negative (FN): False negatives are records that the system fails to detect.

The evaluation metrics considered are

1. Accuracy, which is defined as the proportion of correct results to total inputs.
2. Precision, which indicates the percentage of correct positive detections.
3. Recall, which is the percentage of true positives that were successfully identified.
4. F1 Score, which calculates the score based on both precision and recall. The F1-score is calculated by taking the harmonic mean of precision and recall. If the F1-score is 1, the best value is 1 and the lowest value is 0.

780 normal profiles and 20 artificially made clone profiles were fed to the modules for clone profile detection to see how well they detected clone profiles from the given set. The modules functioned properly and were able to detect clones with reasonable accuracy. The performance of Clone Detection utilising Similarity Measures and C4.5 is shown in Table I, respectively.

PERFORMANCE EVALUATION OF CLONE DETECTION USING C4.5

Total no. of records checked	**800**
No. of normal records detected by system as normal (TN)	765
No. of normal records detected by system as clone (FN)	15
No. of clone records detected by system as normal (FP)	4
No. of clone records detected by system as clone (TP)	16

Tables I demonstrate that similarity metrics were used to find 18 of the 20 clones, whereas the C4.5 classification system only found 16 clones.As a result, clone detection using similarity measurements yields better results than clone detection using the C4.5 classification system.

V.CONCLUSION

Fake and clone profiles have become a very serious problem in online social networks. We hear some or the other threats caused by these profiles in everyday life. So a detection method has been proposed which can find both fake and clone Twitter profiles. For fake detection, a set of rules were used which when applied can classify fake and genuine profiles.

In this research, we proposed an approach for detecting fake accounts on Twitter social network, the proposed approach was based on determining the effective features for the detection process. The attributes have been collected from different research, they have been filtered by extensive analysis as a first stage, and then the features have been weighted. Different experiments have been conducted to reach the minimum set of attributes with perceiving the best accuracy results. From more than 22 attributes, the proposed approach has reached only seven effective attributes for fake accounts detection. Although we claim that these attributes can succeed in discovering the fake accounts in other social networks such as Facebook with minor changes according to the unique nature of each social network, however, we need to prepare a dataset to prove our claim. Moreover, providing an analysis to the tweets content of the user can provide more accurate results in the detection process.

REFERENCES

1. Sowmya P and Madhumita Chatterjee ," Detection of Fake and Cloned Profiles in Online Social Networks", Proceedings 2019: Conference on Technologies for Future Cities (CTFC)
2. Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P.Markatos, "Detecting Social Network Profile Cloning", 2013
3. Piotr Bródka, Mateusz Sobas and Henric Johnson, "Profile Cloning Detection in Social Networks", 2014 European Network Intelligence Conference
4. Stefano Cresci, Roberto Di Pietro, Marinella Petrocchi, Angello Spognardi, Maurizio Tesconi, "Fame for sale: Efficient detection of fake Twitter followers", 2015 Elsevier's journal Decision Support Systems,Volume 80
5. Ahmed El Azab, Amira M Idrees, Mahmoud A Mahmoud, Hesham Hefny, "Fake Account Detection in Twitter Based on Minimum Weighted Feature set", World Academy of Science, Engineering and Technology, International Journal of Computer and Information Engineering Vol:10, 2016
6. M.A.Devmane and N.K.Rana, "Detection and Prevention of Profile Cloning in Online Social Networks", 2014 IEEE International Conference on Recent Advances and Innovations in Engineering
7. Kiruthiga. S, Kola Sujatha. P and Kannan. A, "Detecting Cloning Attack in Social Networks Using Classification and Clustering Techniques" 2014 International Conference on Recent Trends in Information Technology
8. Buket Erşahin, Ozlem Aktaş, Deniz Kilinç, Ceyhun Akyol, "Twitter fake account detection", 2017 International Conference on Computer Science and Engineering (UBMK)
9. Arpitha D, Shrilakshmi Prasad, Prakruthi S, Raghuram A.S, "Python based Machine Learning for Profile Matching", International Research Journal of Engineering and Technology (IRJET), 2018
10. Olga Peled, Michael Fire, Lior Rokach, Yuval Elovici, "Entity Matching in Online Social Networks", 2013 International Conference on Social Computing
11. Aditi Gupta and Rishabh Kaushal, "Towards Detecting Fake User Accounts in Facebook", 2017 ISEA Asia Security and Privacy (ISEASP)
12. Michael Fire, Roy Goldschmidt, Yuval Elovici, "Online Social Networks: Threats and Solutions", JOURNAL OF LATEX CLASS FILES, VOL. 11, NO. 4, DECEMBER 2012, IEEE Communications Surveys & Tutorials
13. Ashraf Khalil, Hassan Hajjdiab and Nabeel Al-Qirim, "Detecting Fake Followers in Twitter: A Machine Learning Approach" 2017 International Journal of Machine Learning and Computing
14. Mohammad Reza Khayyambashi and Fatemeh Salehi Rizi, "An approach for detecting profile cloning in online social networks" 2013 International Conference on e-Commerce in Developing Countries: with focus on e-Security
15. Mauro Conti, Radha Poovendran and Marco Secchiero, "FakeBook:Detecting Fake Profiles in On-line Social Networks", 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining