International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 116-121 June 2018-Dec 2018 www.csjournals.com

A Survey on Automatic Detection of Fake Profiles in Online Social Networks

Bharti[1], Mr. Rajesh Yadav[2]
[1]Student, Assistant Professor[2]
Computer Science, Gurgaon Institute of Technology and Management, Bilaspur, India

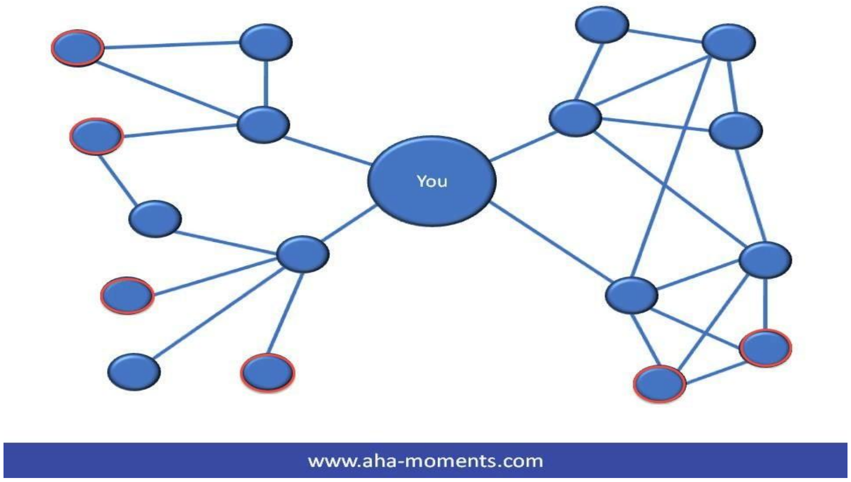
bhartigulyani789@gmail.com, rajesh_libra83@yahoo.com

Abstract: This paper presents the study of various methods for detection of fake profiles. In this paper a study of various papers is done, and in the reviewed paper we explain the algorithm and methods for detecting fake profiles for security purpose. The main part of this paper covers the security assessment of security on social networking sites. On-line Social Networks (OSNs) are increasingly influencing the way people communicate with each other and share personal, professional and political information. Increasing reports of the security and privacy threats in the OSNs is attracting security researchers trying to detect and mitigate threats to individual users. With many OSNs having tens or hundreds of million users collectively generating billions of personal data content that can be exploited, detecting and preventing attacks on individual user privacy is a major challenge. Most of the current research has focused on protecting the privacy of an existing online profile in a given OSN. The fake profile could be exploited to build online relationship with the friends of victim of identity theft, with the final target of stealing personal information of the victim, via interacting online with the friends of the victim. In this paper, we report on the investigation we did on a possible approach to mitigate this problem.

Keywords: Objective, Problem detection, Scope, Conclusion, Survey.

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 who have the same interests. These Online Social Networks (OSN) 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. There are no feasible solution exist to control these problems. In this project, we came up with a framework with which automatic detection of fake profiles is possible and is efficient framework uses classification techniques like Support Vector Machine, Nave Bayes and Decision trees to classify the profiles into fake or genuine classes. As, this is an automatic detection method, it can be applied easily by online social Networks which has millions of profiles whose profiles cannot be examined manually.



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. In the present generation, the social life of everyone has become associated with the online social networks. These sites have made a drastic change in the way we pursue our social life. Adding new friends and keeping in contact with them and their updates has become easier. The online social networks have impact on the science, education, grassroots organizing, employment, business, etc. Researchers have been studying these online social networks to see the impact they make on the people. Teachers can reach the students easily through this making a friendly environment for the students to study .

Related Work

A number of fake account detection approaches rely on the analysis of individual social network profiles, with the aim of identifying the characteristics or a combination thereof that help in distinguishing the legitimate and the fake accounts. Specifically, various features are extracted from the profiles and posts, and then machine learning algorithms are used in order to build a classifier capable of detecting fake accounts .
For instance, the paper Nazir et al. (2010) describes detecting and characterizing phantom profiles in online social gaming applications. The article analyses a Facebook application, the online game “Fighters club”, known to provide incentives and gaming advantage to those users who invite their peers into the game. The authors argue that by providing such incentives the game motivates its players to create fake profiles. By introducing those fake profiles into game, the user would increase incentive value for him/herself. At first, the authors extract 13 features for each game user, and then perform classification using support vector machines (SVMs). The paper concludes that these methods do not suggest any obvious discriminants between real and fake users.

Adikari and Dutta (2014) describe**[2]** identification of fake profiles in LinkedIn. The paper shows that fake profiles can be detected with 84% accuracy and 2.44% false negative, using limited profile data as input. Methods such as neural networks, SVMs, and principal component analysis are applied. Among others, features such as number of languages spoken, education, skills, recommendations, interests, and awards are used. Characteristics of profiles, known to be fake, posted on special web sites are used as a ground truth.

Chu et al. (2010)**[7]** aim at differentiating Twitter accounts operated by human, bots, or cyborgs (i.e., bots and humans working in concert). As a part of the detection problem formulation, the detection of spamming accounts is realized with the help of an Orthogonal Sparse Bigram (OSB) text classifier that uses pairs of words as features. Accompanied with other detecting components assessing the regularity of tweets and some account properties such as the frequency and types of URLs and the use of APIs, the system was able to accurately distinguish the bots and the human-operated accounts.

Wang et al.**[6]** (2012) describe the operational structure of crowdturfing systems, by both crawling the websites used for coordinating crowdturfing campaigns, and by executing a similar, though benign campaign of their own. The authors have found these campaigns to be highly effective in hiring users, and, given the growth in their popularity, they thus pose a serious threat to security.

De Cristofaro et al. (2014) analyse Facebook like farms by deploying honeypot pages. Viswanath et al. (2014) detect black-market Facebook accounts based on the analysis of anomalies in their like behavior.

Farooqi et al. (2015) investigate two black-hat online marketplaces, SEOClerks and MyCheapJobs.

The idea of detecting (dis)similarities in user behavior was also explored in the work by Egele et al. **[5]**(2015). Albeit focusing on interaction over email messages rather than through social networks, the authors nevertheless strive to detect spearphishing by profiling individual email writers and then recognizing whether a new coming email does really originate from the same profile.

Proposed Framework

On this project we presented a machine learning & natural language processing system to observe the false profiles in on-line social networks. Moreover, we are adding the SVM classifier and naïve bayes algorithm to increase the detection accuracy rate of the fake profiles.

The presented process used Facebook profile to notice false profiles. The working method of the proposed procedure includes three principal phases;

1. NLP Pre-processing

2. Principal Component Analysis(PCA)

3. Learning Algorithms

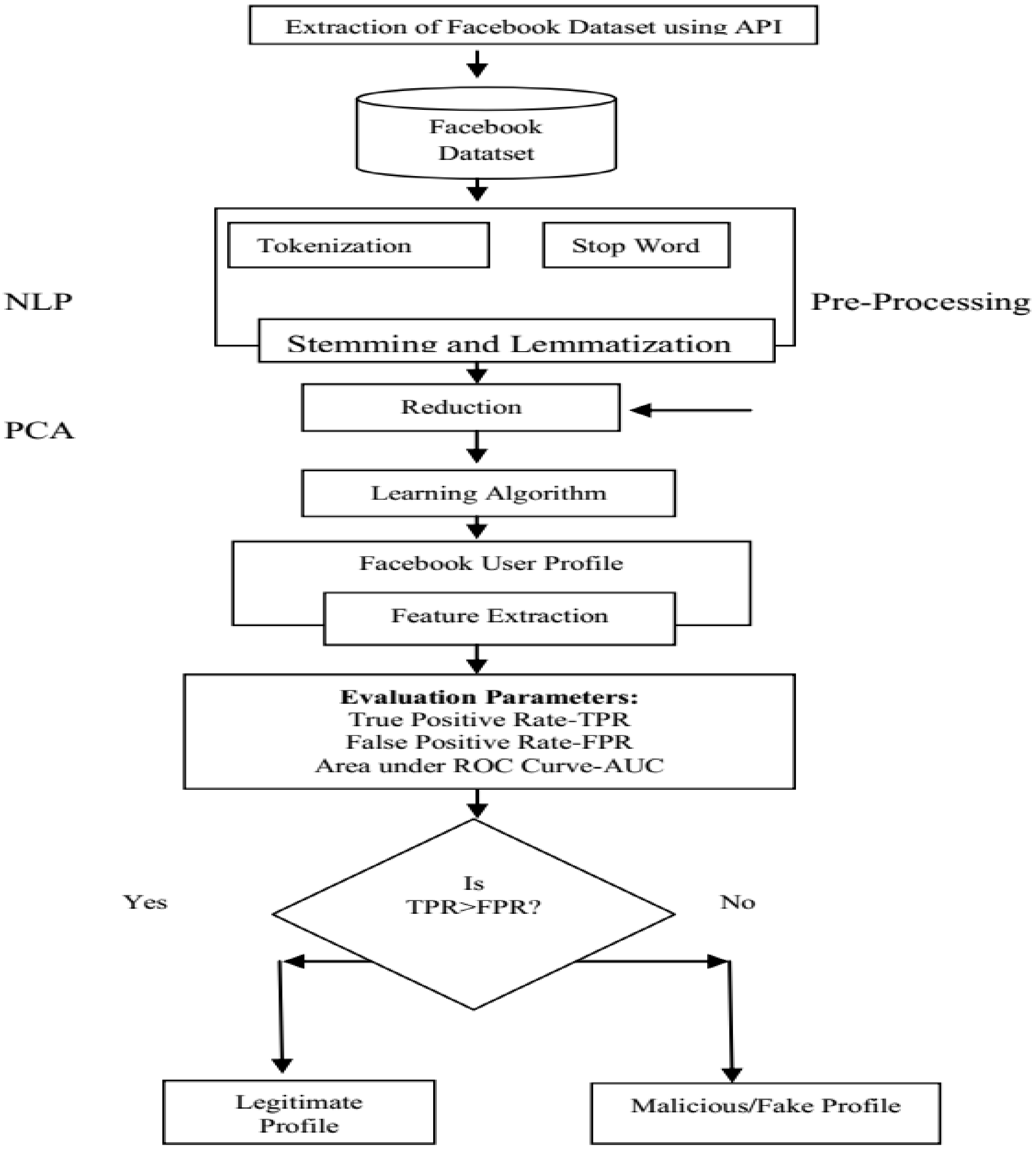
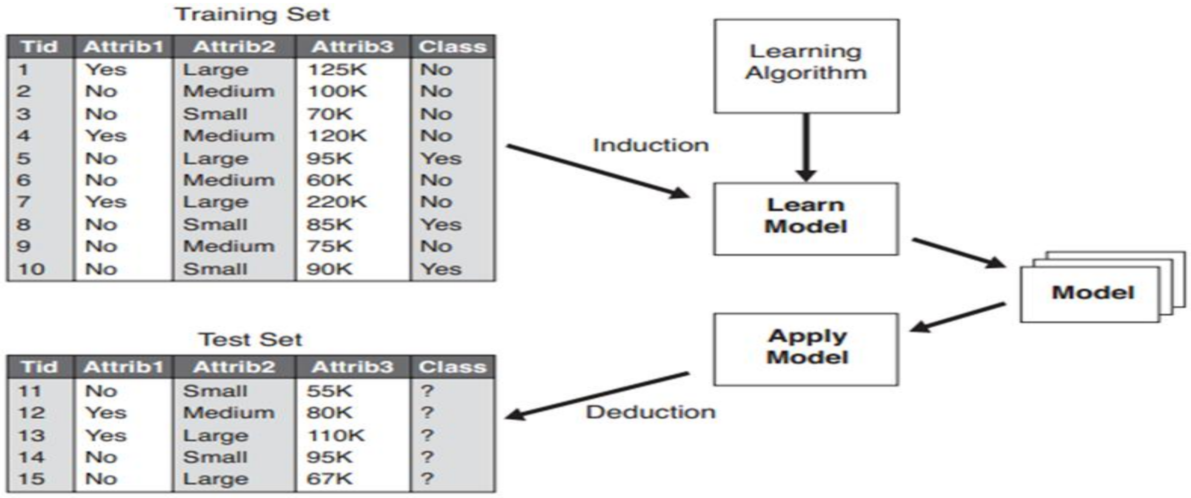


Fig 3.2 Working Procedure for Proposed System

Classification or learning algorithms

In this we are going to use two types of learning algorithms. 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 shows the general approach for building a classification model.



Training Set

Tid	Attrib1	Attrib2	Attrib3	Class
1	Yes	Large	125K	No
2	No	Medium	100K	No
3	No	Small	70K	No
4	Yes	Medium	120K	No
5	No	Large	95K	Yes
6	No	Medium	60K	No
7	Yes	Large	220K	No
8	No	Small	85K	Yes
9	No	Medium	75K	No
10	No	Small	90K	Yes

Test Set

Tid	Attrib1	Attrib2	Attrib3	Class
11	No	Small	55K	?
12	Yes	Medium	80K	?
13	Yes	Large	110K	?
14	No	Small	95K	?
15	No	Large	67K	?

Figure : General approach for building a classification model

The classifiers that we have implemented for classifying the profiles are:

- Naive Bayes Classification
- Decision Tree Classification
- Support Vector Machine

Conclusion and Future Work

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. As future work, we plan to extend our characterization to the on line interactions among the users (tags, friendship requests, rate of requested friendships which are accepted, etc.) and consequently also link strength, to improve the quality of our mechanism.

REFERENCES

[1] 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.

[2]Adikari, S., Dutta, K., 2014. Identifying Fake Profiles in Linkedin, in: PACIS 2014 Proceedings. Presented at the Pacific Asia Conference on Information Systems.

[3] 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.

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

[5] Egele, M., Stringhini, G., Kruegel, C., Vigna, G., 2015. Towards Detecting Compromised Accounts on Social Networks. IEEE Trans. Dependable Secure Comput. PP, 1–1. doi:10.1109/TDSC.2015.2479616.

[6]Chu, Z., Gianvecchio, S., Wang, H., Jajodia, S., 2010. Who is Tweeting on Twitter: Human, Bot, or Cyborg?, in: Proceedings of the 26th Annual Computer Security Applications Conference, ACSAC ’10. ACM, NewYork, NY, USA, pp. 21–30. doi:10.1145/ 1920261.1920265.

[7] 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.