Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technolog

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 02, February-2018

Study on various techniques to detect fake users in Social network

Shruti Varmora

ME, Computer Engineering, GEC-Gandhinagar, Gujarat, India

***Abstract* -** *Internet activities have various communication ways and Social networking is one of the most popular way, with millions of users from around the world. And now a days people spent lots of time on social sites like twitter, Facebook or LinkedIn, and the scenario of using social sites for communication is constantly increasing at an impressive rate. At the same time, users describe their online profile with their personal information that completely represent their accurate identity, and using their profile they interact with other users and perform various activities like content sharing, news reading, posting messages, product reviews and discussing events etc.*

So as the number of users of social networking sites and e-comers sites are impressively increasing and as they have millions of interaction between them, so it would be difficult to identify genuine users and their respective post among them. There various techniques used to detect suspicious accounts, like Trust Model for multimedia social network is useful to detect the suspicious accounts responsible for posting fake multimedia contents.

***Keywords*:** *Trust Model, OSN, DFA*

1. INTRODUCTION

social networking sites has the prelim importance for communication in today's world. In web based services Users are allow to create a public or semi public profile within a community or a group. articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system.

Creating fake profiles or stolen the legitimate user's identity by fraudsters against a number of popular social networking sites is a critical issue now a days. There are various types of user accounts which are not the legitimate users, like Cloned Profiles, Compromised Profiles, Sock Puppets, Sybil Accounts, Bots etc[2].

Users must be aware about that they are with legitimate users not with fake ones, To communicate in any social relationships, internet intruders has favourable activity to Attack OSNs for Example, in Profile Hijacking the intruder can stole the existing legitimate user's profile and obtain the control over them within OSN platform. In Profile Attacking intruder control the existing user's profile and collect their information about OSN activities. For gathering multimedia information Retrieval and Analysis attack is another malicious behaviour. However OSN platforms have to deal with various types of attacks but Sybil attacks are the most usual and practical attacks among them. In Sybil Attack, the fraudsters stolen the identity of real users and pretend to be the same across OSN and without the aware of a specific user or a specific community they obtain their trust.

So to detect such type of fake profiles There various techniques used to detect suspicious accounts, like clustering, classification, finite automata and Trust Model. Various classifiers are used in classification technique. And trust model for multimedia social network is useful to detect the suspicious accounts responsible for posting fake multimedia contents. here is the brief explanation of various methodology which are used to detect fake profiles in social networks. Like Clustering, Classification, finite Automata, trust Model.

2. VARIOUS TECHNIQUES TO DETECT FAKE PROFILES

2.1 Clustering

Clustering is a type of approach which is used to finding group of fake accounts. So identify those groups which include fake accounts it can consider various parameters to detect their identity. For example the group of

account which are created by same account considered as fake accounts, and it may create with some specific reasons like to promote or demote any organization.
To classify those entire clusters of accounts which are legitimate or fake researchers used the technique which is called supervised machine learning pipeline. For example consider detection technique used some feature related to user-generated text. User's personal information is an example of user generated text e.g. name of user, company or university, email Id; these include patterns frequencies within the cluster (e.g., do all of the emails share a common letter/digit pattern) and text comparison frequencies across the entire cluster (e.g., all of the user names are frequent or rare?).

2.2 Classification

To detecting fake users in social network there are various technique used, like supervised learning, semi-supervised learning and unsupervised learning techniques. Unsupervised learning is most probably used for clustering. Using this technique we can compare the user profiles as well as this are also used to detect spam reviews in promotion or demotion of social network websites or for any product. For these classification various classifier are used like neive bayes, SVM(Support Vector Machine) and Dicision tree.

2.3 **Finite automata approach**

This is another technique to detect fake profiles. OSN platforms have to deal with various types of attacks but Sybil attacks are the most usual and practical attacks among them. In Sybil Attack, the fraudsters stolen the identity of real users and pretend to be the same across OSN and without the aware of a specific user or a specific community they obtain their trust. In this Attack, Unfortunately, in OSNs platforms except the traditional mechanisms such as CAPTCHA OSNs have not strong authentication mechanisms for protecting user's profiles against Sybil profile attack. Researchers introduced various approaches methodologies and solutions for detecting Fake Accounts, but these approaches don't perfect solution for this problem. So for advancement in this research, author of this paper present a novel detection technique called Fake Profiles Recognizer (FPR). There are two key approaches of this proposed detection methodology are: Regular Expression and Deterministic Finite Automaton (DFA)[3]. To identify and verify user profiles in OSNs, proposed methodology of this paper is based on some formulated hypothesis:
1)In the social graph each node should be represented using a unique Regular Expression; author of a proposed paper called it "a Friend Pattern (FP)".
2) Using a predefined friend pattern, each friend is marked with an instance of this pattern in the friend list.
3) In the social graph each node is incorporated with a pre-designed Deterministic Finite Automaton (DFA) and friend pattern derived an instance and this DFA verify the instance identity.
4) So In specific profile the fake identity visible as a cloned profile from the users friend list.
So identity of profiles is identified and recognizes using the detection mechanism called FPR. FPR has the key functionality: to represent the identity of user profile as friend pattern using Regular Expression approach and to recognize the identity of profiles as Friend Pattern Processor using Deterministic Finite Automaton approach.

2.4 Trust Model

- **Trust Factor used in communication of social network**

User of social networking sites has more concern about their Privacy. Number of members and their interactions has direct effect of privacy on them. For ease of communication open nature of the social networks is important but as the privacy of the users is critical issue, to build *trust communities* is important.
A community which is created by considering their members privacy and security so that they can gives their opinion, share their thoughts, and talks about their experience in an open and honest way without the fear of being judge, this type of community is called trust community. Social network trust models introduced various terms to calculate trust are ***social trust*** and ***social capital***.
There two features of trust: ***Popularity Trust*** **(PopTrust)** and ***Engagement Trust*** **(EngTrust)**. In trust communities acceptance and approval of a member by other members is Popularity trust, while involvement of someone in the community refers to the engagement trust. In community a member's trustworthiness is considered as popularity trust and how much a member trusts other members in the community is considered as engagement trust.
• Proposed paper introduced a novel framework using social capital and recommendation system for building *trust communities* in social networks.
• for of building trust communities It propose a novel *social trust* model, called *STrust*, for social networks.

• Unlike other trust models, there are some social trust model is based on the principles of social science and derived using social capital.
•Social trust model of this proposed paper separates the interactions of user in a social network into two groups popularity based interactions and engagement based interactions, these two groups of interaction of trust model is recognize passive interactions. e.g reading comments without leaving any feedback is a passive interaction.
A model for social trust, called *STrust*, is defined based on individual members' popularity and engagement in the community.

- **Trust Model for Multimedia Social Network**

There is various social network applications which are established for the use of communication. But as the security concern building trust in between users and in community is most important issue now a day. Researchers established Multimedia social network (MSN), a network application of the typical small world theory. MSN was established based on trust relationship between people in a realistic society. MSNs provided a platform where users share their digital content based on a certain relationship of trust, and maintaining their social relations network for users. On the sharing and transmission mode of digital contents trust relationship of users has direct effect. Therefore, in order to correctly evaluate trust relationship between users and minimize security threats in the sharing process, proposed work introduced Creditability of users and their historic information about previous interaction. Multimedia social networks trust model (MSNTM) based on small world theory can be used for detection of fake profile. And to check the effectiveness of the trust model researchers uses a simulation experiment for the same purpose.

3. CONCLUSION

Privacy and security of a individual's profile is primary concern of social networking site for communication. But, As users are gradually increasing in social and e-comers site now a days. This is tedious job to identify legitimate users and to detect fake profiles. Detection of trusted profiles are important for safe and useful communication. This paper proposed various methodologies which are useful for detection of suspicious account.

4. ACKNOWLEDGEMENT

I grateful to all my advisors for their expertise and endless helpful advice, and me guide to support me and advice me. I also thankful to all the authors and reviewers for their comments and feedback to my work. Work is done under the expert opinion and guidance.

REFERENCES

[1] Mauro Conti, Radha Poovendran, Marco Secchiero, "FakeBook: Detecting Fake Profiles in On-Line Social Networks", 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, added to IEEE Xplor on 4th Feb 2013.
[2] Cao Xiao, David Mandell Freeman, Theodore Hwa, "Detecting Clusters of Fake Accounts in Online Social Networks", University of Washington and. LinkedIn Corporation, oct 16,2015

[3] Mohamed Torky, Ali Meligy, Hani Ibrahim, "Recognizing Fake identities in Online Social Networks based on a Finite Automaton approach", computer Engineering Conference(ICENCO), 2016- 12th international, 28-29 Dec, 2016, Added to IEEE Xplor on 16th feb 2017.

[4] Jitendra Kumar Rout, Smriti Singh, Sanjay Kumar Jena1, Sambit Bakshi1, "Deceptive review detection using labelled and unlabeled data", Multimedia Tools And Applications on February 2017.

[5] Surya Nepal, Cecile Paris, Vanita Sherchan, "Surya Nepal, Cecile Paris, Vanita Sherchan",

[6] Zhiyong Zhang • Kanliang Wang, "A trust model for multimedia social networks", Social Network Analysis and mining on December 2013.

[7] Todd Bodnar, Conrad Tucker, Kenneth Hopkinson, Sven G. Bil´en, "Increasing the Veracity of Event Detection on Social Media Networks Through User Trust Modeling",

[8] Sajid Yousuf Bhat & Muhammad Abulaish," Communities Against Deception in Online Social Networks", *Communities Against Deception in Online Social Networks, Computer Fraud and Security, 2014, Elsevier, Feb. 2014.*

[9] Mudasir Ahmad Wani*, Suraiya Jabin, “A sneak into the Devil’s Colony- Fake Profiles in Online Social Networks”

[10] Simon Fong, Yan Zhuang, Maya Yu, Iris Ma, “Quantitive analysis of trust factors on Social Networks using data mining Approach”, 2012- IEEE
[11] M. Daiyan1, Dr. S. K.Tiwari2, M. A. Alam3, “Mining Product Reviews for Spam Detection Using Supervised Technique”, International Journal of Emerging Technology and Advanced Engineering, August 2014.
[12] Sahil Puri1, Dishant Gosain, Mehak Ahuja, Ishita Kathuria, Nishtha Jatana,
“Comparison And Analysis Of Spam Detection Algorithms” IJAIEM, April 2013
[13] Michail Tsikerdekis, “Identity Deception Prevention using Common Contribution Network Data”, IEEE,2015
[14] Guowei Wu1, Zuosong Liu1, Lin Yao1,∗ , Jing Deng2 and Jie Wang, “A Trust Routing for Multimedia Social Networks”, The Computer Journal Advance Access published October 4, 2014.
[15] **Ali M. Meligy, Hani M. Ibrahim, Mohamed F. Torky,** A Framework for Detecting Cloning Attacks in OSN Based on a Novel Social Graph Topology, *I.J. Intelligent Systems and Applications,* 2015,
[16] Lijun Yang, Zhiyong Zhang, Weili Tian, Qingli Chen, “Advance on Trust Model and Evolution Method in social network”, 2012 Sixth International Conference on Genetic and Evolutionary Computing.
[17] http://www.yourarticlelibrary.com
[18]https://www.scribd.com /doc/14790526/Trust-Models
[19] Data Mining Concepts and Techniques/third Edition/ Jiawei Han, Micheline Kamber, Jian Pei
[20] Data mining/ Practical machine Learning Tools and Techniques/ Ian H. Written and eibe frank