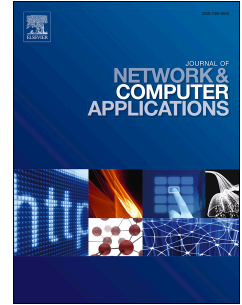# Accepted Manuscript

Rise of spam and compromised accounts in online social networks: A state-of-the-art review of different combating approaches

Ravneet Kaur, Sarbjeet Singh, Harish Kumar

Please cite this article as: Kaur, R., Singh, S., Kumar, H., Rise of spam and compromised accounts in online social networks: A state-of-the-art review of different combating approaches, *Journal of Network and Computer Applications* (2018), doi: 10.1016/j.jnca.2018.03.015.

Rise of Spam and Compromised Accounts in Online Social Networks: A State-of-the-Art Review of Different Combating Approaches

Ravneet Kaur, Sarbjeet Singh, Harish Kumar

University Institute of Engineering and Technology, Panjab University, Chandigarh, India

ravneets48@gmail.com, sarbjeet@pu.ac.in, harishk@pu.ac.in

Abstract

Ever increasing fame and obsession for social networks has also coxswained a dramatic increase in the presence of malicious activities. As a result, various researchers have proposed different features and techniques to detect and reduce this menace. This paper presents an expository study of various state-of-the-art techniques to detect two most interlinked apprehensive problems on social networks namely, spam detection and detection-cum-analysis of compromised accounts. It is evident from the ongoing statistics that despite profuse awareness and some anti-spam policies and techniques being developed, to everyone's surprise, the severity of spam has only increased. Moreover, with the growing smartness of spammers, existing techniques get bypassed and new features and techniques continuously keep on evolving. Therefore, in continuation to the ongoing research, a study comprising of a comprehensive analysis of different works is also required from time to time. The growing inclination of spammers to compromise the legitimate accounts has evolved as an evasive and more beneficial way to spread spam. Therefore, it has become highly relevant to review the techniques related to the detection of compromised accounts so as to track the spammers adhering to this behavior. In this work, we have performed a qualitative analysis of each paper discussing its pros and cons. In both the domains, the detection approaches have been placed under different categories and have been thoroughly reviewed stating their applicability. In conclusion, the paper carries a discussion of various gaps prevalent in the existing approaches and the corresponding actions to be taken to address them, providing a strong foundation for future researches to be carried out in this domain.

Keywords: Social networks, security, malicious activities, spam, spam campaigns, compromised accounts, classification, clustering

1. Introduction

Online social networks act as a communication platform where different users with a personalized user profile interact and share information with each other. Due to the growing trend and increasing popularity of such networks, there has been a sudden inclination of people towards the use of these sites. A recent survey reflects that around 2 billion internet users are using various social networking platforms which amount to 71% of the total internet population[1]. Also, among the popular social networks such as, Facebook, Twitter, Instagram, Pinterest, Sina Weibo etc., Facebook surpassed others in terms of popularity and number of users with 1.6 billion users across the globe followed by Twitter with 1.3 billion registered users **[1, 2]**. Moreover, every second, five new profiles are being created on Facebook [2] and it is reported that many of the created profiles are just bots, fake, dormant or compromised. As per a year back survey conducted by **Parsons [3]**, it is found that roughly 170 million accounts on Facebook are fake and most of them are automatically created using some softwares. The count was 83 million in 2012 which rose to 140 million in 2014 and then 170 million presently [2] thus making it a tedious issue, which with time is becoming cumbersome for service providers to handle. Another Facebook statistics from 2012 state that out of 83 million fake Facebook accounts, 1.5% accounts are intentionally created to spread spam and perform other malicious activities **[4]**.

Above statistics infer that albeit an alarming increase in the use of social networking sites, the security and privacy aspect of these platforms still need a lot of improvements. Recently, people have started petitioning Facebook, LinkedIn, and other social networks to stop identity thefts and the creation of fake accounts **[5]**. Moreover, users have started quitting social network platforms because of the reasons such as, privacy risks, addiction to Facebook, dissatisfaction with Facebook's services, etc., out of which privacy issues being the prime (48%)**[6]**. Thus, the inability to attract new users or retain the existing ones may pose a threat to the business and financial aspects of a company, because of which it has become extremely necessary for service providers to provide required security to the users. Ethically, it is the duty of social network service providers to provide full privacy and security to the users, but many a times, they themself team up with advertisement companies to populate the user's personal information and behavior patterns. As an example, **Krishnamurthy and Wills [7]** described how many of the popular

---

[1] http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[2] https://zephoria.com/top-15-valuable-facebook-statistics/