Scholar's Name: Mudasir Ahmad Wani

Supervisor's Name: Dr. Suraiya Jabin

Department: Department of Computer Science (Faculty of Natural Science)

Thesis Title: Fake Profile Detection in Online Social Networks

Abstract

Online Social Network (OSN) is an online platform used by people to create social, personal or professional relations with other OSN users who share similar interests, activities, backgrounds or real-life connections. In the light of graph theory, an OSN is visualized as the grouping of nodes (individuals, actors, organizations, etc.) connected by a set of edges (relationships, interactions, distances, etc.). OSNs have changed the way people think, express, and socialize with the outside world. With the Web technology 2.0, several Online Social Networks (OSNs), such as Facebook, Twitter, LinkedIn, Instagram, Researchgate, etc. have been developed with a variety of functionalities. These OSNs are used by people to carry out their social as well as professional activities. Since the structure of OSNs bears a resemblance to the real-life communities, and they hold a massive amount of user content, therefore, they are highly important to the researchers and several other disciplines including marketing, sociology, politics, etc.

Apart from researchers and business organizations, the universal popularity of OSNs has also attracted the attention of cybercriminals. These cybercriminals exploit the exposure and weakness of an OSN to perform unlawful, misleading, malicious, or discriminatory operations. They penetrate the social network either by creating fake profiles or by executing a number of identity theft attacks like cloning attacks, spoofing attacks, etc. A growing number of hackers are creating forged identities on networks like Facebook and Twitter in order execute unlawful activities such as access the social as well as personal information of users, to promote a particular brand or a person, to defame a user, etc. Several researchers have proposed different fake profile detection approaches. Unfortunately, with the time these adversaries adapt new strategies and bypass the detection systems which are yet a challenge for researchers. Another challenge faced by researchers working in this direction is the unavailability of ground truth data. No benchmark dataset for fake profiles on *Facebook* has been released so far and collecting it manually makes the task complex and time-consuming. For efficient fake profile detector, one must prepare an appropriate and effective feature set. The features can be either observed manually from the social network sites or explored using literature survey. However, it is also possible that some of the features existing in literature may not prove to be fruitful at present as the adversaries keep on changing their behavior to fool and bypass detection systems.

In this thesis, initially we aim to put everything related to online fake profiles at one place by presenting various categories of fake profiles like compromised profiles, cloned profiles and online bots (spam-bots, social-bots, like-bots and influential-bots) on different OSN sites along with different category of features to distinguish fake entities from real ones. We also addressed the challenge of data unavailability by providing extremely obliging data collection techniques along with some existing data sources. After the rigorous survey of the literature, we proposed an iMacros technology-based data crawler to collect the data from user profiles on the Facebook social network. We performed behavior and emotion analysis on the collected data and observed how people share their thoughts on the social media. Based on the four profile features ($work(w)$, $education(e)$, $home\_town(ht)$ and $current\_city(cc)$) along with a network feature ($Mutual\ Clustering\ Coefficient\ (M_{CC})$) we proposed an approach to identify suspicious (negative) links established by the adversaries by exploiting the mutual friend feature in a group or a page on $Facebook$. The three classification techniques ($Decision\,Tree, SVM\ and\ Naive\ Bayes$) have shown better results on the test dataset. After performing the emotion analysis of users on the Facebook network, we proposed a fake profile detection model that incorporates sentiment-based attributes to differentiate real and fake OSN profiles on the network. The experiments are conducted on the posts of Facebook users. The detection model is trained on 12 emotion-based attributes including Plutchik's eight basic *emotions, positivity, negativity, number of emotions categories and emotion variance*. Finally, four supervised machine learning algorithms, SVM, Naïve Bayes (NB), JRip and Random Forest were used to train the proposed model. Random Forest delivered the best result for all three metrics, accuracy, F-measure and AUROC.

The $Mutual\ Clustering\ Coefficient\ (M_{CC})$-based suspicious link identification system model can be used by the OSN service providers to alert their members with a list of suspicious connection (links) from their respective friend lists so that users can themselves verify the suggested links and filter their friend list as per their requirement. Apart from assisting the OSN users and service providers in identifying the suspicious links on the network, the proposed approach can be employed by the researchers to design efficient fake profile detection systems. Furthermore, it can also be utilized to identify the weaker and stronger ties of a user. Although the proposed approach has been tested for $Facebook$ users, with the little modifications, it will be applicable to other social networking sites as well.

Furthermore, the presented emotion analysis conducted in this thesis has been carried out only on the text content present in the user posts. However, the analysis can be extended to study emotions revealed in the images and videos shared by a user. Furthermore, the work can be extended to include sarcasm and emoticons analysis to gather the accurate sentiments of the posts.