PhD Project

Semi-supervised Deep Learning Approach for Spam Detection in Multi-layered Social Networks

Online social network platforms have become part of the daily lives of more than a billion individuals. They are used for a variety of activities like socialization, information, ebusiness and self-promotion. This increasing use of social networking platforms has raised the need to develop automated methods for their analysis. One of the most common data-mining task performed on social networks is user's classification with wide range application. It allows detecting malicious users, spammer or malware distributors.

Social data is characterized by a wide variety of attributes that stem from posting habits in addition to interactions. Collective classification considers not only the attributes of a given user but also attributes of users he interacted with in order to decide on the label to assign to him. This high number of attributes requires the use of efficient attribute selection and weighting methods that could be provided by a deep learning framework [1].

Deep learning allows the generation of models that capture the complex patterns linked to the behavior of suspicious nodes on social networks. It helps to identify the correlations between a node's posting behavior and its neighbor's habits. This has been successfully used in an unsupervised mode to learn the structural patterns of interaction in graphs using random walks to generate features [2]. It has also been applied in a supervised mode in a variety of learning tasks based on textual attributes [3].

Very few works explored deep learning in a semi-supervised mode with the aim of capturing both textual and structural patterns in a social network. This method could reveal important patterns that would allow increasing the accuracy of classification for a variety of tasks. Using input data for learning purposes could reduce the effects of one of the main drawbacks of deep learning, which is the need for a large labeled training dataset. The use of structural and text attributes would allow reducing the noise introduced in a semi-supervised mode due to mislabeling in the training set. Finally, the use of a rich feature set composed of both textual and structural features would increase the accuracy of classification due to capturing unique patterns that could only stem from the analysis of both modes.

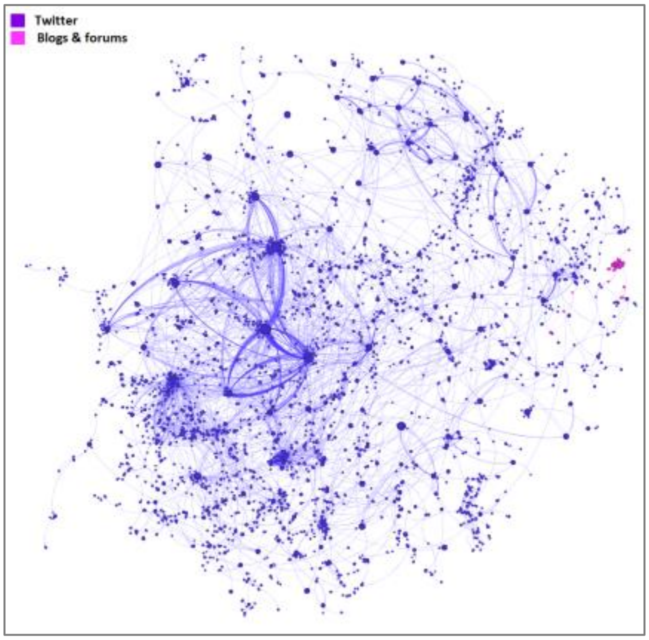

Figure 1: Source Omar Jaafor and Babiga Birregah. 2015. Multi-layered graph-based model for social engineering vulnerability assessment. In Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015 (ASONAM)

The aim of this thesis is to provide a fast and reliable algorithm to analyze multi-layered social network ([4]) for spam detection using deep learning technique in a semi-supervised approach.

Babiga BIRREGAH, Assistant Professor. Laboratoire de Modélisation et Sûreté des Systèmes (LM2S), Département Recherche Opérationnelle, Statistiques Appliquées, Simulation (ROSAS)
12, rue Marie Curie, CS 42060 - 10004 Troyes Cedex. Email : babiga.birregah@utt.fr, Tél. : (+33) 03 25 71 58 69

More specifically this research will aim at:
1- making a state of the art of deep learning technics in the context of social networks analysis,
2- proposing a framework which rely on the use of deep learning in semi-supervised machine learning algorithm to detect behavioral outliers
3- using the proposed framework to identify cybercrim activities such as spam detection on social networks

Joint research programme:

This project will conducted in the frame of a joint supervision between the LM2S team of University of Technology of Troyes and the Internet Commerce Security Laboratory (ICSL), a research unit of Federation University Australia.
The successful candidate will spent half of his time in both the two university.

References

[1] Aminanto, M. E., & Kim, K. (2016, August). Detecting Impersonation Attack in WiFi Networks Using Deep Learning Approach. In *WISA* (pp. 136-147).
[2] B. Perozzi, R. Al-Rfou, and S. Skiena, “DeepWalk: Online Learning of Social Representations,” 2014. [Online].
Available: http://arxiv.org/abs/1403.6652%0Ahttp://dx.doi.org/10.1145/2623330.2623732
[3] J. Schmidhuber, “Deep Learning in neural networks: An overview,” Neural Networks, vol. 61, pp. 85–117, 2015.
[4] Jaafor, O., & Birregah, B. (2017). Social Engineering Threat Assessment Using a Multi-Layered Graph-Based Model. In *Trends in Social Network Analysis* (pp. 107-133). Springer International Publishing.
[5] Omar Jaafor and Babiga Birregah. 2017. Collective classification in social networks. In Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017 (ASONAM '17), Jana Diesner, Elena Ferrari, and Guandong Xu (Eds.). ACM, New York, NY, USA, 827-835.