Title: Malicious Social Bot Detection: RL-RNN based Hybrid Approach

Author: Palagiri Swathi, Mousumi Karmakar, Sumit Kumar Banshal, Raka Moni

Abstract: This paper proposes a new method called RL- RNN that combines the power of Reinforcement Learning and Recurrent Neural Networks in furthering malicious bot detection. Malicious social bots on Twitter have emerged as a significant threat to this platform, spreading disinformation, manipulating public opinion, and influencing political events. The existing traditional detection methods, such as Support Vector Machines, are proven to be unable to deal with bot behaviors dynam- ically and complicatedly. The proposed model inculcates that URL features with frequency and patterns of postings are hot indicators of bot activity. The RL component enables the model to adjust dynamically to changing bot behaviors. It also adapts the RNN type to capture the sequential structure of the tweets with the associated URLs. Thus, experimental results show that this approach using RL- RNN hybrids significantly outperforms traditional SVM-based methods by precision, recall, and overall detection accuracy. The experimental results point out the RL- RNN model's ability to scalability in detecting evolving bot strategies on Twitter. This makes the approach more effective as a mitigation method for preventing malicious activities, thus increasing security in social media systems.

Keywords: Malicious Social Bots, Twitter Network, Rein- forcement Learning (RL), Recurrent Neural Network (RNN), Support Vector Machine (SVM), URL Features, Bot Detection

DOI: https://doi.org/10.1109/DELCON64804.2024.10866368

https://www.researchgate.net/publication/388913265