Abstract

The Online Social Networks (OSN) have a great role in increasing the communication among people. Their role never stops as they have become the way to share information and the real-time news. However, their unprecedented success has also attracted the attention of hackers, who use OSN to spread spam and malicious contents. Hackers have found a good environment, which is compatible with their goals in terms of widespread reach to the largest number of victims or even spreading large propaganda in a very short time. All this can be done using OSN. The presence of spam and malicious contents on OSN may lead to people’s aversion from these sites. This research tackles this phenomenon by introducing Flexible Malicious Accounts Detector (FMAD) solution, which can detect malicious and spam accounts using predefined features. Additionally, FMADA can identify newly emerging features and classify them as either normal or abnormal. Moreover, FMADA can recognize malicious accounts campaigns. Therefore, the presented solution performs better than all previous approaches that cannot deal with new emerging features. For this purpose, FMAD uses both supervised and unsupervised machine learning techniques. The experiment shows that FMAD results in
Flexible Malicious Accounts Detector (FMAD) for Mining Twitter Social Network using Features and Accounts Frequent Pattern accuracy reaching 99.75 %.

References


Index Terms

Computer Science  Security

Keywords

OSN; Spam; Malicious account detection; datamining; Association rules.