Sequence-Based Features And Statistical Relational Models

Posted on March 14, 2019

Introduction

There are different methods that can be used to determine spammers and malicious activities. These methods include graph structure features, sequence-based features, and statistical relational models. Thus, all these methods can help identify spammers needing manual or automated intervention (Ahmed et al., 2014). Therefore, the multi-national nature assists spammers with more options but improves the detection mechanisms to limit patterns across the task types and time. Apart from the use of graph features, one could use sequence-based features as well as a statistical model.

Sequence-Based Features

The sequence method is used in different domains, such as biology, detection of malicious activities, and information retrieval. Thus, it can be used for computational prediction and detection. In changing multi-relational social networks, every individual using a social network generates a sequence which can be detected by this method. Thus, spammers normally use particular objectives in the social network, and this causes their sequence of behaviour to diverge from their norm (Ahmed et al., 2014). These sequences include sequential k-gram features and Mixtures of Markov Models. The model multi-national nature assists spammers with more options but improves the detection mechanisms to limit patterns across the task types and time.

Sequential k-gram features

The easier way to represent a series with the feature is to recognize that each element in the series is independent of the others. But this doesn’t make it possible to identify the order of the sequence. Also, treating each element independently it implies that values in the sequence will not change as the out-degree in each vertex. Therefore, in order to identify the order of the sequence, the K-gram is used. The sequence is taken as a vector of frequencies. To enable us to keep the feature computationally effective, we use the bigram sequence, i.e., k=2. The K-gram helps identify spammers who need a manual or automated intervention like a graphical feature.

A mixture of Markov Models

Although the k-gram feature helps in attaining an order of events in sequence, it may fail to outline this order properly in longer sequences. This is because the increasing K alters the feature space, which leads to computational inefficiency and estimation problems due to feature gaps. Therefore, to identify the sequence order in a longer series and to predict the information, we use a generative model. This model is the same as the chain-augmented Bayes model, which has proven to be efficient in information modelling (Huang et al., 2013). Like graph features, the model's multi-national nature assists spammers with more options but improves the detection mechanisms to limit patterns across the task types and time. Thus, the model identifies the actions of each social network user through a mixture of Markov models. Therefore, each class of spammer has a relationship with a feature y. Thus, it is assumed that component y is generated from a Markov particular class.

Statistical Relational Model

Hinge-loss Markov Random Fields

Hinge-loss Markov random Fields (HL-MRFs) include models that are conditional and probabilistic continuous (Huang et al., 2013). These models are log-linear, whose components are the hinge-loss activity of the variable's states. They are made and based on soft logic, and they can be used to generalize logical implications. The function takes potentials and random variables as well as conditioned variables. Thus, it takes the following function:

Hinge-loss Markov Random Fields Collective Model for Reports

The objective of this model is to utilize reports to forecast spammers. Thus, Hinge-loss Markov, Random Fields Models, help to incorporate users' credibility information in the report and help in improving the predictability of the given reports (Huang et al. 2013). By using this, we show that group reasoning over the reliability of the informing user and his or her probability of being a malicious user helps in increasing the performance of the system. This approach may use graph relation to report and is founded on the belief that the reliability of the user's abuse reporting should have a higher probability of being a spammer. Thus, if the user report is not likely to be a spammer, the reliability of the reporting should decrease and vice versa.

Use of Time Window

Graph features use a multi-national nature to give spammers more options, but they also improve detection systems to control patterns across time. Thus, the representation of the social network users' is instructed by time-stamped data. Therefore, the author produces a graph using a time

window. The author uses the sequence of the users' information to identify the occurrence of malicious activity in using a social network. The time is used to determine the reliability of the user's report. As the use of social networks evolves, each user produces a sequence of behaviours or activities which are measured by time (Gao, 2010). The time will help determine the intentions of the user. The test time is computed by the posterior probability of the user and the recorded activity of the sequence.

Conclusion

Therefore, rather than graph features, one could use sequence-based features and statistical relational models. Although the graph feature is widely used, the named models can effectively and efficiently be used to increase the performance of the system. Thus, all these methods can help identify spammers who need manual or automated intervention. Therefore, the multi-national nature assists spammers with more options but improves the detection mechanisms to limit patterns across the task types and time. Sequence-based features and statistical models can be used to achieve the same results as graph features. Graph features use a multi-national nature to give spammers more options, but they also improve detection systems to control patterns across time. Therefore, the author produces a graph using a time window.

References

Ahmed, N. K., Neville, J., & Kompella, R. (2014). Network sampling: From static to streaming graphs. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, *8*(2), 7.

Gao, H., Hu, J., Wilson, C., Li, Z., Chen, Y., & Zhao, B. Y. (2010, November). Detecting and characterizing social spam campaigns. In *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement* (pp. 35-47). ACM.

Huang, B., Kimmig, A., Getoor, L., & Golbeck, J. (2013, April). A flexible framework for probabilistic models of social trust. In *International conference on social computing, behavioral-cultural modeling, and prediction* (pp. 265-273). Springer, Berlin, Heidelberg.

Spirin, N., & Han, J. (2012). Survey on web spam detection: principles and algorithms. *ACM SIGKDD Explorations Newsletter*, *13*(2), 50-64.