Using a Data Mining Approach: Spam Detection on Facebook

M. Soiraya, S. Thanalerdmongkol, C. Chantrapornchai
Department of Computing, Faculty of Science
Silpakorn University, Thailand, 73000

ABSTRACT

In this work, we present a social network spam detection application based on texts. Particularly, we tested on the Facebook spam. We develop an application to test the prototype of Facebook spam detection. The features for checking spams are the number of keywords, the average number of words, the text length, the number of links. The data mining model using the decision tree J48 is created using Weka [1]**.** The methodology can be extended to include other attributes. The prototype application demonstrates the real use of the Facebook application.

General Terms

Data Mining, Web Application, Social Networking, Decision Tree.

Keywords

Social network;Spam dection;Data minig; Facebook application.

1. INTRODUCTION

Data mining has been used in many applications recently [2]. It has been used for classification, identification, prediction, finding association etc. It is also combined to existing applications such as inventory/stock forecasting, image classification, spam classification and so on.

In this work, we study the potential application on detecting spams on social network using data mining. We particularly develop a prototype system that detects the spam on the Facebook. The application is running on the server where the Facebook request is rerouted to it to process the spam checking. We use the decision tree model J48 for classification. Sample 150 posts are trained and 75 posts and tested on the model. The features used are the number of words, the length of the post, and the number of the links with the recall rate of 66%.

Currently, there are several methods that detect spam patterns using data mining [3].

1. Anamaly detection. This is a way to detect an abnormal behavior among all typical case data.

2. Associative learning. It is like Amazon book suggestion. Typical users that have a behavior may perform the other more behaviors.

3. Cluster detection. The data is clustered in a group using some similarity threshold or criteria.

4. Classification. If we know the classification beforehand, we may categorize the given data into classes.

5. Regression. It is a prediction model. Based on the history data, the future behavior may be predicted using the model.

There are many works that study spam detections in various ways. For example, the work in [4] [5] [6] studied spam emails and images in emails. Some works inspect on the spam images only like [7] which use the decision tree method. Wang et.al. used image feature filtering to detect image spam [8] Many works until now focused on the web spam [9] [10]. The web link was investigated as the web spam or not [11]. In [12], improper web access detection was presented. The work demonstrated the usage of the proxy server with the blacklist, whitelist, keyword blocking. Jin, Lin, Luo and Han presented the framework called SocialSpamGuard. It is a spam detection system for social networks. The framework models the media network as a graph. The features are inspected such as image content, texts, and social network features to indicate the spam behaviours [13].

In [14],the framework for spam detection is also presented. The work is based on the HITS web link method and the bipartite graphs. The scores are calculated and semi-unsupervised learning was used to model. Also, in [15] social spam detection is proposed with six features such as plagiarism, valid link, number of advertisements, unrelated tags, tag spams, contents of sources etc.

Typical data mining technique for spam detections are as following [16].

1. Keyword search. This considers the documents that match the query best. Usually, TFIDF is calculated.
2. Linked-based ranking. The approach ranks the links. The popular algorithm is Pagerank or HITS.

In the above literature, there are also other features that are useful for counting such as term frequency, inverse document frequency, hyperlinks to documents etc. Normal data mining consist of two major steps: model construction where the model is created using a training set data and model testing where the test set is used to test the accuracy of the model.

To construct the model, the features of the problem need to be investigated thoroughly. Then the classification algorithm is used to derive the model. In this paper, we use the decision tree J48 as a prototype model for the classification. The selected attributes are the number of keywords, the number of links, the length of the post, the average number of words in a post. The relationships of the attributes may further be investigated in the future. The goal of this work is to only demonstrate the use of data mining model in detecting spams in the Facebook application.

The paper is organized as follows. The next section presents some backgrounds and theory in data mining. Section 3 presents our methodology. Section 4 presents the model results and application architecture. Section 5 concludes the paper.

2. BACKGROUNDS

We present parts of the theories and technology used in the work.