AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Binary Bat Approach for Effective Spam Classification in Online Social Networks

R.R.Rajalaxmi and A.Ramesh

Department of Computer Science and Engineering, Kongu Engineering College, Perundurai, Erode-638052, Tamil Nadu, India

ARTICLE INFO

Article history:
Received 19 August 2014
Received in revised form
19 September 2014
Accepted 29 September 2014
Available online 3 December 2014

Keywords:
Facebook, Feature selection, Binary Bat, Genetic Algorithm, Classification

ABSTRACT

Background: Social Network Mining is the most emerging area in the Data Mining. Now a days predicting spammers in online social networking sites had become a difficult challenge due to large number of features. In the recent existing works only the dependency of each feature from the face book towards classification is analyzed and there was no work to identify minimum number of features to classify. In the proposed work, a binary bat approach is employed to select the best features. This method performs feature selection based on the echolocation behaviour of bats. For experimental purpose we have collected real data from Facebook profile of different users containing normal and spam profiles. The results of the proposed approach is compared with standard feature selection algorithms. To classify the profiels we have used JRip classification algorithm. The results show that the binary bat approach gives the best results when compared with other methods.

To Cite This Article: R.R.Rajalaxmi and A.Ramesh., Binary Bat Approach for Effective Spam Classification in Online Social Networks, ***Aust. J. Basic & Appl. Sci.,*** *8(18): 383-388 2014*

INTRODUCTION

Due to increasing popularity of social media, Online Social Networks (OSNs) have become a popular communication and information sharing tool over the past few years. The users of the social networks are the key role players and they are responsible for the contents being shared in the networks. Online Social Network Mining is an area for extracting the knowledge from various kinds of data of the social networking sites, so that we can understand the behaviour of the users of Online Social Network sites.

Facebook is an online social networking service. It was founded on February 4, 2004 by Mark Zuckerberg with his friends. Facebook allows anyone who claims to be at least 13 years old to become a registered user of the website. Users must register before using the site, after which they may create a personal profile, add other users as friends, exchange messages, and receive automatic notifications when they update their profile. Facebook has a number of features with which users may interact. The features are Walls, Pokes, Photos, Status, News feed, Like button. Facebook users have had the ability to make live voice calls via Facebook Chat, allowing users to chat with others from all over the world.

Individual users of the social network shares his/her personal information among a group of trusted people (Thomas *et al.* 2011). Other users also belief the infomarion available in their network. This makes the malicious users of the network to spread spam messages. Usually spammers exploit the trusted network by promoting advertisements, personal blogs, phising and scam. These people utilize the services of social networks to disseminate bogus messages. In this work, spam detection in facebook profiles is addressed. Our study is based on real datasets collected from Facebook that contain both ham and spam profiles. We have identified a set of 18 statistical features of Facebook. Next, a binary bat approach is used to detect relevant features of spam profiles.

Related Work:

Online Social Networking works (OSNs) have become a popular communication and information sharing tool over the past few years due to increasing popularity of social media (Benevateuo and Roudrigues,2009). The users of the social networks are the key role players and they are responsible for the contents being shared in the networks. The individual users are the basic elements in the hierarchy of OSN, and the next elements are the communities formed by friends, families and acquaintances. Users share information by sharing links to interesting websites, videos and files. The feature of sharing information to a large number of individuals with

Corresponding Author: R.R.Rajalaxmi, Department of CSE, Kongu Engineering College, Perundurai, Erode-52, TamilNadu, India
E-mail: rrr_kec@yahoo.co.in

ease has attracted malicious parties, including social spammers. Social spammers exploit the network of trust for spreading spam messages promoting personal blogs, advertisement, phishing and scam. Spammers employ different strategies for getting into a user's network of trust.

Gao *et al* (2010) studied the detection of social spam campaigns with a large anonymized dataset of asynchronous "wall" messages between Facebook users. To make a spam campaign effective, they modelled each wall post as a <destination, URL> pair. Validation methodology includes a series of steps, each of which encapsulates a different tool and aims to concretely verify some portion of the suspicious wall posts which are malicious. They investigated the false positive rate of the proposed methodology by re-examining the malicious wall posts. Three different formats (hyperlinks, plaintext and obfuscated text) are used to embed URL in wall posts. Finally the result show that attackers are actively leveraging the "ready-made" friend links of compromised accounts for spam, and clearly show that online social networks are now a major delivery platform targeted for spam and malware delivery.

Jin *et al* (2011) applied a data mining concept for spam detection system in social media networks. Business entities or public figures set up social networking pages to enhance direct interactions with online users. Social media systems heavily depend on users for content contribution and sharing. One of the major challenges of spam detection in social media is that the spam is usually in the form of photos and text. To identify spam photos they extract the image content features as color histogram, color correlogram, gabor features etc., where as text features are extracted from image-associated content, such as caption, description, comments and URLs.

Stringhini *et al* (2010) detect the spammers on social networking using honey profiles. Unfortunately, social networking sites do not provide strong authentication mechanisms and it is easy to impersonate a user and sneak in to person's network of trust. The important characteristic of social network is the different levels of user awareness with respect to threats. Finally the result show that it is possible to automatically identify the accounts used by spammers based on the statistical analysis where users spend more times on popular social networking site than any other sites but spammers use more than the normal users.

Ahmed and Abulaish (2013) presented a generic approach to detect spam profiles on different categories of OSN. Their study was based on real datasets collected from Facebook and Twitter networks that contain both benign and spam profiles. To classify the spam profiles they have used three classification algorithms namely, decision tree (J48), rule-learner (Jrip) and Naive Bayes (NB). Their analysis on individual features shows that features related to friends/followers, pages or tags and URLs are important for classification. Removing such a feature from the dataset results in reduced detection accuracy which is due to misclassification of certain instances. They also reveal that some features provide critical information about profile's behaviour.

Khoshgoftaar *et al* (2013) compare a study of iterative and non-iterative feature selection techniques for software defect prediction. The two important problems which affect the performance of classification models are high-dimensionality and imbalanced data. The Threshold Based Feature Selection (TBFS) technique was proposed by the team and implemented in weka tool. TBFS procedure includes two steps: (1) normalizing the attribute values so that they fall between 0 and 1; (2) treating those values as the posterior probabilities from which to calculate performance metrics.

Qiwei *et al* (2014) discussed the prediction of self-monitoring skills using textual posts on Facebook. The popularity of the Social Networking Site Facebook has grown unprecedented during the past five years. The research question investigated is whether posts on FB would also be applicable for the prediction of user's psychological traits such as Self-Monitoring (SM) skill that is supposed to be linked with user's expression behaviour in the online environment. They present a model to evaluate the relationship between the posts and SM skills. The aim of the study is twofold where first, evaluate the quality of responses to the Snyder's Self-Monitoring Questionnaire collected via the internet and secondly, to explore the textual features of the posts in different SM-level groups.

Based on the literature survey for spam detection in social networks, it is found that several features contribute to the identification of spam. Thus it is essential to identify the most promising features relevant to spam (Peng *et al*, 2005). Hence, selecting relevant features from the facebook profiles for spam classification can be formulated as a feature selection problem. However, it is categorixed as an optimization problem since the solution space representing the problem is huge in size (Roudrigues *et al*, 2014). An optimization problem is the problem of finding the best solution from all feasible solutions. The approximate solution for these problems can be found by using algorithms based on Swarm Intelligence. An optimization algorithm is an iterative procedure, starting from an initial guess. Algorithms like Particle Swarm Optimization (PSO), Ant Colony Optimization(ACO), Firefly Algorithm (FA), Bat Algorithm (BA) and Bee Algorithm fall in this category. These algorithms should have two key components as exploitation and exploration, which are also referred to as intensification and diversification. Despite the huge number of studies about various swarm intelligence based algorithms, BA seems to get more attention now-a-days.

Australian Journal of Basic and Applied Sciences, 8(18) December 2014, Pages: 383-388

As many techniques are used to find the spam campaigns in online social network, it does not deal with filtering of features. In order to further improve the accuracy with minimum number of features, swarm intelligence based optimization algorithms can be used.

Proposed Work:

A. Bat Algorithm:

Bats are fascinating animals and their advanced capability of echolocation has attracted attention of researchers from different fields. Bats emit a loud and short pulse of sound, wait until it hits into an object and, after a fraction of time, the echo returns back to their ears. Thus, bats can compute how far they are from an object. In addition, this amazing orientation mechanism makes bats being able to distinguish the difference between an obstacle and a prey, allowing them to hunt even in complete darkness. This behaviour of bats has been mathematically modeled in Bat Algorithm (Roudrigues *et al*, 2014). In BA, an artificial bat has a position vector, velocity vector, and frequency vector which are updated during the course of iterations. In the BA, the artificial bats can move around the search space utilizing the position and velocity vectors (or updated position vectors) within the continuous real domain.

Each bat has a positon (xi), frequency (fi) and velocity (vi) in a d-dmensional search space. To move to the next position it is updated with new velocity at each iteration as follows:

$$v_i(t+1) = v_i(t) + (x_i(t) - gbest)\, f_i \tag{1}$$

Where gbest is the best solution obtained so far. The position of the bat is now updated as follows:

$$x_i(t+1) = x_i(t) + v_i(t) \tag{2}$$

The frequency of each bat is computed at each iteration as follows:

$$f_i = f_{\min} + (f_{\max} - f_{\min})\beta \tag{3}$$

where β is a radom number uniformly distributed in the range [0,1]. In order to improve the explotation capability of BA a random walk is employed as given below:

$$x_{new} = x_{old} + \varepsilon A^t \tag{4}$$

where ε is a random number between [-1,1] and A is the loudness of emiited sound. At each iteration, the loudness and pulse emission rate are adjusted as follows:

$$A_i(t+1) = \alpha A_i(t) \tag{5}$$

$$r_i(t+1) = r_i(0) + [1 - \exp(-\gamma t)] \tag{6}$$

where α and γ are constants.

B. Binary Bat algorithm:

In a Binary Bat algorithm, the new bat's position is of binary values. A binary search space can be considered as a hypercube. The search agents (particles) of a binary optimization algorithm can only shift to nearer and farther corners of this hypercube by flipping various numbers of bits. Hence, in designing the binary version of BA, some basic concepts of the velocity and position updating process must be modified. In a binary space, due to dealing with only two numbers (''0'' and ''1''), the position updating process cannot be performed same as in normal bat algorithm. Therefore, a transfer function (Roudrigues *et al*, 2014) can be used for changing agents' positions from ''0'' to ''1'' or vice versa. Figure 1 depicts the proposed binary bat algorithm. The following sigmoid function is used for updating the bat position in the binary space:

$$s(v_i^k) = \frac{1}{1 + e^{-v_i^k}} \tag{7}$$

where v_i^k is the velocity of the bat i in kth dimension. Now the position of the bat is modified as

$$x_i^k = \begin{cases} 1 & if\ s(v_i^k) > \sigma \\ 0 & if\ s(v_i^k) \le \sigma \end{cases} \tag{8}$$

where σ is uniformly distributed between [0,1].Once the features are selected using the bats, their fitness have to be evaluated. In order to accomplish this, the following fitness function is used:

$$fitness(x_i) = 100 - Acc(x_i) \tag{9}$$

where Acc(xi) denotes the accuracy of the bat obtained using JRip classifier[18]. To validate the classification results, 10-fold cross validation is used.

Dataset Description:

Facebook consist of many features like Walls, Posts, Status, News feed, Tags, like button (Sung-um *et al* 2014). Wall is a space on every user's profile page that allows friends to post messages for the user to see. Poke allows users to send a virtual "poke" to each other (a notification tells a user that they have been poked Status, which allows users to inform their friends of their whereabouts and actions). Depending on privacy settings,

Australian Journal of Basic and Applied Sciences, 8(18) December 2014, Pages: 383-388

anyone who can see a user's profile can also view that user's Wall. News Feed, which appears on every user's homepage and updates the information including profile changes, upcoming events, and birthdays of the user's friends.

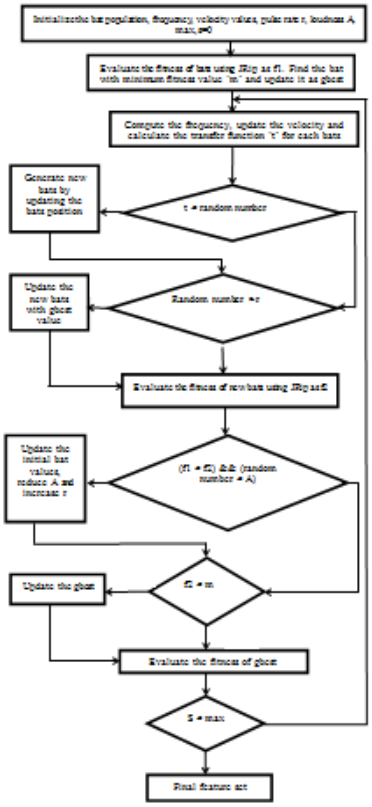

Fig. 1: Proposed Binary Bat Algorithm.

Facebook allows users to upload an unlimited number of photos, compared with other image hosting services like Photo bucket and Flickrb(Thomas *et al*, 2011). Another feature of the Photos application is the ability to "tag", or label users in a photo. For instance, if a photo contains a user's friend, then the user can tag the friend in the photo. This sends a notification to the friend that they have been tagged, and provides them a link to see the photo. The like button is a social networking feature, allowing users to express their appreciation of content such as status updates, comments, photos, and advertisements.

In this work 18 features from the Facebook profiles are used. Data collection is done by logging into the users profile. On the Timeline page, by clicking on the "Activity log" button the timeline pages of each profile is downloaded. Each feature data from the timeline profiles between 2010-2013 for 201 users are manually counted and the csv file of the dataset is prepared. Table 1 describes the dataset features.

Table 1: Dataset description.

S.NO	FEATURE	DESCRIPTION
1	Friends	No of Friends
2	Community pages	No of community pages liked by the user
3	Total post by user on community pages	Total post by the user on his/her community pages
4	Maximum status on his/her wall	Maximum status update made by the user
5	Post rating	Rating given to the user based on their total status
6	Total post on friends wall	Total no of post by the user on his/her friends wall
7	Maximum status on friends wall	Maximum status update made by the user on friends wall
8	Post rating	Rating given to the user based on their total status posted on their friends wall
9	Total url	Total url shared by the user
10	Unique url	Total no of unique url shared by the user
11	Repetition url	Repetition frequency of the url
12	Total tag	Total no of post the users are tagged
13	Tagged users	Total no of users tagged in the post
14	Rating tag	Rating given to the user based on tagging feature
15	Group	Total no of groups the user belongs
16	Events	Total no of events the user attended
17	Apps	Total no of Facebook apps used by the user
18	Likes	Total no of post the user liked

Australian Journal of Basic and Applied Sciences, 8(18) December 2014, Pages: 383-388

Experimental Results:

In this section a thorough evaluation of identified features of Facebook data using binary bat approach is presented. Here, five different classification algorithms namely JRip, J48, Naïve Bayes, k-NN, SVM (Wittan *et al*, 2005) are used to establish the discriminative properties of the identified features to classify spam and ham profiles. JRip classifier gives the best results for the Facebook data. Table 2. shows the parameters used in BBA.

Table 2: Parameters used.

PARAMETER	VALUE
No. of bats	10
Loudness	0.25
Pulse rate	0.5
Classifier	JRip
Maximum iterations	50

Figure 2 shows the result for feature selection of Facebook dataset using the BBA. Initially ten bats are populated and it is evaluated using JRip classifier. The random values are generated and they are used by the bats. For fifty iterations frequency of the bats are calculated and velocity is updated and position of the bats are updated by calculating transfer function. New bats are generated and they are evaluated using JRip classifier. In the first iteration, six features are selected with 99.00% accuracy and upto eighth iteration same features remain. During the nineth iteration, maximum accuracy of 99.50 % with 9 best features is achieved. From nineth iteration to fiftieth iteration the same features remains stagnant with the same 99.50% accuracy. The features selected at the fiftieth iteration are No_Friends, Max_post, Total_post_Friends, Maximum_status_Friends, Rating_post_Friends,Repetition_url, Total_tags, Groups and Events. Thus these features are treated as the best features.

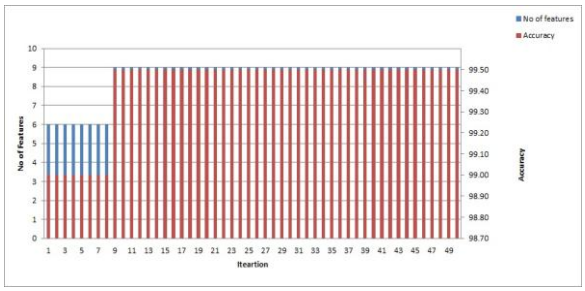

Fig. 2: Feature selection using BBA.

Figure 3 depicts the comparative results of BBA with other feature selection algorithms. While comparing BBA with other feature selection algorithms like forward feature selection, forward feature inclusion, backward elimination feature selection and iterative feature selection, it is observed that BBA gives the maximum 99.50% accuracy with nine features.The features selected from BBA are No_Friends, Max_post, Total_post_Friends, Maximum_status_Friends,Rating_post_Friends, Repetition_url, Total_tags, Groups and Events. Though minimum number of features are obtained as a result of other algorithms, the features selected as a result of BBA are very much related to the features used for manual classification of facebook profiles.

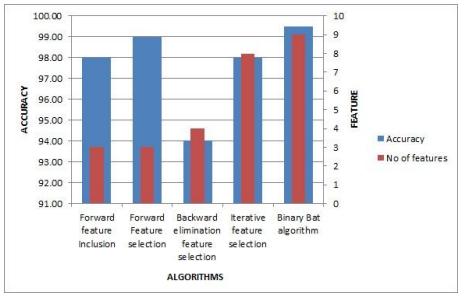

Fig. 5: Comparison of BBA with other feature selection algorithms.

Conclusion:

Predicting Spammers in Facebook is a difficult task. In this work, different features related to facebook profile is considered to predict spam. Then binary bat approach is implemented to select relevant features for spam classification. The proposed BBA achieves maximum accuracy of 99.50% with nine features. Though minimum numbers of features are obtained as a result of other approaches, the features selected as a result of

BBA are very much related to the features used for manual classification of face book profiles. The features obtained due to the application of BBA algorithm is similar to those features obtained during manual inspection of facebook profile. In future, extra features from the facebook can be added and other optimization algorithms can be used to predict the spammers in social networking sites.

REFERENCES

Ahmed, F. and M. Abulaish, 2013. "A generic statistical approach for spam detection in Online Social Networks".Computer Communications, 36: 1120-1129.

Benevenuto, F. and T. Rodrigues,"Characterizing user behaviour in online Social networks", in Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement, ACM, 49-62.

Debahuti, M., R. Amiya Kumar, A. Milu and J. Tanushree, 2009. "A hybridized method for feature selection in gene expression", Computer Communication Technology,11: 85-98.

Gao, H., J. Hu, C. Wilson, Z. Li, Y. Chen, Ben, Y. Zhao, 2010. "Detecting and Characterizing Social Spam Campaigns",IMC'10, 1-3. Melbourne, Australia.

Jin, X., C.X. Lin, .J Luo and J. Han, 2011. "A Data Mining based Spam Detection System for Social Media Networks",Proceedings of the VLDB Endowment, 4: 12 Seattle, Washington.

Khoshgoftaar, T.M., K.G.A. Napolitano and R. Wald, 2013. "A comparative study of iterative and non-iterative feature selection techniques for software defect prediction". Springer Science, Business Media, DOI 10.1007/s10796-013-9430-0, New York.

Liu & Yu, 2005. "Toward integrating feature selection algorithm for classification", IEEE Trans. Knowledge Data Eng., 17(4): 491-503.

Nakamura, R.Y., L.A.M. Pereria, K.A. Costa, D. Rodrigues, J.P. Papa, X.S. Yang, 2012. BBA: A binary bat algorithm for feature selection, Intenrational conference on graphics, patterns and images, 291-297.

Peng, H., F. Long, F.C. Ding, 2005."Feature selection based on mutual information: Criteria of max dependency, max-relevance and min- redundancy", IEEE Trans. Pattern Anal. Mach. Intell, 278: 1226-1239.

Qiwei He, Cees, A.W. Glas, Michal Kosinski, David, J. Stillwell, Bernard, P. Veldkamp, 2014. "Predicting self-monitoring skills using Textual posts on Facebook", Computers in Human Behaviour, 33: 69-78 .

Roudrigues, D., A.M. Perireia, Y.M. Nakamura, A.P. Kosta, X. Yang, A.N. Souza and J.P. Papa, 2014. "A wrapper approach for feature selection based on Bat algorithm and Optimum path forest", Expert System with Applications, 14: 2250-2258.

Stringhini, G., C. Kruegel and G.Vigna, 2010. "Detecting Spammers on Social Networks". Dec., 6-10. Austin, Texas USA.

Sung-Bum Kim, Dae-Young Kim, Kevin Wise, 2014. The effect of Searching and surfing on recognition of destination images on Facebook pages, Computers in Human Behaviour, 30: 813-82315.

Thomas, K., C. Grier, V. Paxson and D. Song, 2011. "Design and evaluation of real time url spam filtering service", in IEEE Symposium on Security and Privacy.

Wittan, I.H. and H Ian, 2005. Data Mining:Practical machine learning Tools and Techniques, Morgan Kaufmann Series, Data Management Systems,153-168.

Yang, X.S., 2014."Swarm Intelligence based algorithms:a critical Analysis",Springer-Verlag, 7: 17-28.