Detection and Prevention of Spam Mail with Semantics-based text classification of Collaborative and Content Filtering

S.Prayla Shyry, Y.Bevish Jinila
Assoc Prof, School of computing, Sathyabama Institute of Science and technology
praylashyry@gmail.com, ybevish@gmail.com

Abstract.

Eventhough , conventional technologies are quiet good in separating spam messages, still soo many measures have to be considered to make more accuracy in spam filtering. In this work, we worked towards detecting spam mails and filtering it during its transmission. We proposed Collaborative filtering approach hybrid with text classification (semantics based). The related feature are retrieved from the text content. Also, another filtering method known as Content-based filtering is proposed which filters the same spam mail with more precision and better accuracy. Along with the semantic texts the Content-based filtering filters the special symbols such as HTML tags, @, / etc. Results are compared and the accuracy of detecting spam e-mails of Content-based filters is more than that of Collaborative filters. Both Collaborative and Content-based filters perform keyword check available in the spam keyword database and detects whether the mail sent by the sender is genuine or spam. Genuine emails are sent successfully and the spam emails are blocked at the server side. Content-based email classification requires an understanding of both structural and semantic attributes of email. Conventional research is focussed on semantic properties through structural components of email. After analysing the emails as events (as a major subset of the class of email), a rich contextual test-bed representation for an understanding of the semantic attributes of emails has been devised. The event-based emails have traditionally been studied based on simple structural properties.

Keywords

Collaborative filtering, Content filtering, Semantics-based text classification, Spam Mail.

1. Introduction

Increase in the quantity of spam mails have made tremendous issues in the cybercrime. Also the unaware users are being irritated and cheated by the spammers. Email users are looking for even more spam filter as day by day new spam mails are in their inbox. Still email users are experiencing several spam messages insisting the importance of enhancing the spam filtering even more. Conventional technologies include converting all text to vector space model and as set is framed. Hence the grouping techniques and Machine learning techniques are used to arrange the contents. As machine learning techniques are connected with content based, more specifically SVM and naïve bayes are used to filter the spams. In this paper we focussed on the semantics of the info in the content of the message. We found that other than the words in the content, the semantics of the data gives better result.
In most articles Unsolicited Commercial Email and spam have same meaning. However, people classify emails subjectively as spam based on whether the email is of interest to them rather on whether they adhere to a definition. Even though Server-based collaborative filtering is better in in many systems, it falls since it has the favor in ubiquitous computing settings. Hence we propose a novel approach with Semantics-based text classification of Emails with Collaborative and Content Filtering.

2. Related Works

Aakash et al. (2017) proposed spam classification with focused view on the multiplication of spam messages. In this paper, all the parameters are considered as elements and the order of messages on different parameters are considered. Particularly the messages order dependent on parameters. They also found good results. They proposed the order of messages dependent on different parameters and each parameter remains as a element in machine learning technique. machine learning calculation. Their effort gives better result.

Chae et al. (2017) proposed an efficient spam email classifier with hybrid model. They build the order of messages from spam mails. And build order precision for spam mails. Order of spam mail in spam channel is displayed. Patrice et al. (2018) developed Amavis to do record grouping, private record, associated record. Wuxu et al. (2018) improved the accuracy of the Naive Bayes Spam Filter and detects text modifications and efficiently classified the email as spam or ham.

Ammar et al. (2016) used factual classifiers in the spam channel to find out the crisp or genuine email. They have calculated the false positive and false negative rates and they have reduced the rates by calculating phishing index and ham mails. Hempelmann et al. (2011) proposed semantic-based method and they separated no text and less text with semantics. The semantic is extracted and processed to identify as ham or spam mail. A semantic analyzer gives better result. Qing Yu et al. (2018) used deep dependency trait vectorization with CNN to analyse short text messages. They used dependency parsing and formed a binary tree. A matrix I formed using the arc in binary tree. Eigen vectors were found by decomposing the tree. Their results shows that their model is fast and effective than traditional.

3. Proposed System

Once the email is received, initially it is filtered with collaborative filtering, if the spam is detected, it is blocked. if it is not spam, content based filtering is applied on the mail as a second step verification. After the final check, the spam mail is blocked. And if it is a genuine mail, it is sent to the receiver end.

Fig. 1 Workflow of the proposed system
3.1.1 Collaborative filtering

Collaborative Filtering is the process of filtering information among multiple data sources.

Algorithm for collaborative filtering:

Input: Training, Testing, Individual Agent
Steps:
1. Set the threshold
2. Train the individual agent
3. Find the proper model from training data.
4. Select random individual agents
5. Individual and its weight value are combined
6. Decide the class by comparing the values
7. Find the weight value from the individual agent
8. Update the weight value on the individual agent.
Output: Spam mail

3.1.2 Data flow diagram

In Data Flow Diagram, directed graph nodes represent processing activity and represent data items transmitted between processing nodes.

The user is asked to enter details like username, password, e-mail id, contact details etc. After entering all the details successfully, the system gives successful account creation and the user is able to have a permanent account. User can use the username and password for account log in.
3.1.3 Login Page

The user is asked to enter the admin login id and password. Entering the correct login id and password authenticates the user to send as well as receive e-mails. User need to enter the correct login details otherwise user will not be able to login.

3.1.4 Compose Mail

Here, the administrator can send mail to anyone having registered e-mail id through the below steps:

1. Admin selects the compose mail option.
2. The system returns the format of the mail.
3. Admin enter the user id of the receiver, subject (if any), and messages.
4. The system sends the mail to the intended receiver.
5. If the corresponding user id does not exist, the system gives an error message.
3.1.5 Sent Box

After sending e-mail to another user the respective e-mail is stored in the sent box of the receiver’s account. Sent e-mails are stored in the database stored in the back end of the system.

![Fig 7 Sent Box](image)

3.1.6 Sending Spam Mail

The user sends the e-mail including spam keywords to the receiver and one of the two filters i.e. collaborative and content-based filters is always selected so that the spam mail is filtered and an error message appears saying “Your mail is filtered as spam”. After the spam is detected it is automatically blocked.

![Fig 8 Sending spam mail](image)
4. Spam Blocking

After the spam is detected and filtered from the genuine mails, the corresponding spam mail is then blocked and stored in a separate database. It is stored in database and receiver will not receive mail if it is detected spam.

4.1.1. Collaborative and content Based filtering (Calculating Accuracy)

Accuracy value for filtering spam mails is determined using factors like precision value, F1 measure and recall value. The accuracy for collaborative filters on a particular spam e-mail dataset is shown in Fig 11. As the content-based filters detect the spam attributes more precisely than the collaborative filters. Hence, the accuracy value of content-based filter is more compared to collaborative filters. The accuracy for content-based filters on a particular spam e-mail dataset is shown in Fig 12.
The accuracy for detecting and filtering spam e-mails with respect to various parameters per second is shown below in table 1

| Parameters  | Collaborative Filtering | Content-based Filtering |
|-------------|-------------------------|-------------------------|
| Precision   | 1.0                     | 1.0                     |
| Recall      | 0.40268456375838924     | 0.8456375838926175     |
| F1 score    | 0.077419354838924       | 0.9163636363636364     |
| Accuracy    | 0.8718345116502775     | 1.703650655328964      |

These results show that the Content-based filter’s detection and filtering rate is more precise and accurate as compared to Collaborative filters. This is because Collaborative filters can only filter the spam containing semantic text whereas Content-based filters detect spam even in special characters and symbols.
The above graph shows that the recall value of content-based filtering (0.8456375838926175) is comparatively higher than collaborative filtering (0.40268456375838924).

![Fig. 14 Graphical representation of F1 value](image)

The above graph shows that the F1 value of content-based filtering (0.9163636363636364) is comparatively higher than collaborative filtering (0.077419354838924).

![Fig. 15 Graphical representation of Accuracy value](image)

5. Conclusion and Future Work

Because of the characters of spam issues, massive and continuous, spam filtering approaches with higher performance are still required to be developed urgently. In this work, an effective approach to detect spam e-mails is being implemented which keep spam messages from being exchanged. The extraction of semantic information of text was achieved by attaching semantic annotations on the words and sentences of it. The results of the experiment conducted on the corpus of UCI repository showed a satisfactory performance on detection and prevention of spam texts and indicate enormous potentiality in spam filtering with multiple classes and less feature terms. Spam e-mails are checked through Collaborative filters and then checked in Content-based filters for further filtering. After the spam e-
mail is filtered, it is blocked and prevented to be sent to receiver. Our analysis shows that the accuracy of Content-based filter (1.703650655328964) is higher than that of Collaborative filter (0.8718345116502775). The future efforts would be extended towards: Achieving accurate classification, with zero percent (0%) misclassification of Ham E-mail as Spam and Spam E-mail as Ham. The efforts would be applied to block Phishing E-mails, which carries the phishing attacks and now-days which is more matter of concern. Also, the work can be extended to keep away the Denial of Service attack (DoS) which has now, emerged in Distributed fashion called as Distributed Denial of Service Attack (DDoS).

REFERENCES

[1] Patrice Samuel Rompas, Riza Satria Perdana, “Securing Confidential Documents in Local Network Using an Email Filtering Technique”, 2018 International Workshop on Big data and Information Security (IWBIIS)

[2] Wuxu Peng, Linda Huang, Julia Jia, Emma Ingram, “Enhancing the Naive Bayes Spam Filter through Intelligent Text Modification Detection”, 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications.

[3] Wei Hu, Jinglong, and Yongkang Xing, “Spam Filtering by Semantics-based Text Classification”, 8th International Conference on Advanced Computational Intelligence Chiang Mai, Thailand; February 14-16, 2017.

[4] Aakash Atul Alurkar, Sourabh Bharat Ranade, Shreeya Vijay Joshi, Siddhesh Sanjay Ranade, “A proposed data science approach for email spam classification using machine learning techniques”, 2017 Internet of Things Business Models, Users, and Networks.

[5] Ghulam Mujtaba, Liyana Shuib, Ram Gopal Raj, Nahdia Majeed; Mohammed Ali Al- Garadi, “Email Classification Research Trends: Review and Open Issues”, IEEE Access, 2017, Vol.5, Pg-9044-9064.

[6] Ammar Yahya daeef, R. Badlishah Ahmad, Yasmin Yacob, Naimah Yaakob, Kumurul, Fazira Ku Azir, “Multi Phishing Email Classification”, Journal of Theoretical and Applied Information Technology 20th January 2016, Vol.83, No.2.

[7] Fazira Ku Azir, “Multi Phishing Email Classification”, Journal of Theoretical and Applied Information Technology 20th January 2016. Vol.83. No.2

[8] Dr. S. Prayla Shyry, “Performance in Selfish Overlay Network by Fuzzy Logic Deployment of Over Nodes”, International Conference on Control, Instrumentation, Communication, and Computational Technologies, (IEE Xplore), Pg-717-721, IICC ICT 2014.

[9] B. Trstenjak, S. Mikac, D. Donkeo, “KNN with TF-IDF based Framework for Text Categorization,” Procedural Engineering, 2014, 69(1):1356–1364.

[10] P. W. Foltz, S. Gilliam, and S. Kendall, “Supporting content-based feedback in online writing evaluation with LSA,” Interactive Learning Environments, 2014, pp. 111-129.

[11] C. F. Hempelmann, and V. Mehra, “Baseline semantic spam filtering,” Proceedings of the 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology, 2011, vol. 3, pp.273-276.

[12] J. M. Taylor, C. F. Hempelmann, and V. Raskin, “On an automatic acquisition toolbox for ontologies and lexicons in ontological semantics,” International Conference on Artificial Intelligence, 2010, pp. 863–869.

[13] K. Lee, J. Caverlee, and S. Weeb, “Uncovering social scam: Social nets machine learning,” SIIR, Geneva, 2010, pp. 435–442.

[14] G. Stringhini, C. Kruegel, and G. Vigna, “Detecting spammers on social networks,” in Proc. ACSAC, Austin, Texas, 2010, pp. 1–9.

[15] C. F. Hempelmann, J. M. Taylor, and V. Raskin, “Applied guided ontological engineering,” International Conference on Artificial Intelligence, 2010, pp.843-849.

[16] V. Raskin, C. F. Hempelmann, and J. M. Taylor, “Guessing vs. knowing: The two approaches
to semantics in natural language processing,” Annual International Conference Dialogue, 2010, pp. 642–650.
[17] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, “Sybil: Defining against Sybil attacks via social networks,” IEEE/ACM Transactions on Networking, vol. 16, no. 3, pp. 576–589, 2008.
[18] G. Forman, and E. Kirshenbaum, “Extremely fast text feature extraction for classification and indexing,” Proc of 17th ACM Conference on Information & Knowledge Management, 2008, pp. 1221–1230.
[19] V. Metsis, I. Androutsopoulos, and G. Paliras, “Spam filtering with Naive Bayes”, Proc. of the 3rd CA, 2006, pp. 1–5.