

## Extracting Messages from the Social Networks

ARKALA VIJAY KUMAR<sup>1</sup>, A. RAMESH BABU<sup>2</sup>

<sup>1</sup>PG Scholar, Dept of CSE, JB Institute of Engineering & Technology, India, E-mail: vijjuarukala@gmail.com.

<sup>2</sup>Associate Professor, Dept of CSE, JB Institute of Engineering & Technology, India, E-mail: askarbabu@gmail.com.

**Abstract:** As we know, today everyone is using On-line Social Networks (OSNs) to communicate and share information. Therefore one important need in today On-line Social Networks (OSNs) is to give users the ability to control the messages posted on their own private space to avoid that unwanted content is displayed. OSNs provide little support to this requirement up to now. To provide this, we propose a system allowing OSN users to have a direct control on the messages posted on their walls. This is accomplished through a flexible rule-based system, which allows users to customize the filtering criteria to be applied to their walls, and a Machine Learning based soft classifier which automatically produces membership labels in support of content-based filtering.

**Keywords:** Information Filtering, On-Line Social Networks, Short Text Classification, Policy-Based Personalization.

### I. INTRODUCTION

Today the most popular interactive medium to communicate, share and disseminate a considerable amount of human life information are On-line Social Networks (OSNs). Daily and continuous communications imply the exchange of several types of content, including free text, image, and audio and video data. According to Facebook statistics average user creates 90 pieces of content each month, whereas more than 30 billion pieces of content are shared each month. Information filtering can therefore give users the ability to automatically control the messages written on their own walls, by filtering out unwanted messages. Truly, today OSNs provide very little support to prevent unwanted messages on user walls. For example, Face book lets users to state who is allowed to insert messages in their walls (i.e., friends, friends of friends, or defined groups of friends). However, content-based preferences are not supported. Wall messages are constituted by short text for which traditional classification methods have serious limitations since short texts do not provide sufficient word occurrences. Therefore the aim of the present work is to propose and experimentally evaluate an automated system, called Filtered Wall (FW), able to filter unwanted messages from OSN user walls. The support for content based user preferences is the key idea of proposed system. This is possible thank to the use of a Machine Learning (ML) text categorization procedure [12] able to automatically assign

with each message a set of categories based on its content. Section II reviews related work, whereas Section III presents the conceptual architecture of the proposed system. Section IV describes the ML-based text classification method used to categorize text contents, whereas Section V explains FRs and BLs. Section VI describes the case study. Finally, section VII concludes the paper.

### II. LITERATURE SURVEY

Filtering is based on explanations of individual or group information preferences that typically represent long-term interests. Users get only the data that is extracted. Information filtering systems are intended to categorize a stream of dynamically generated information and present it to the user those information that are likely to satisfy user requirements [1]. In this paper the main focus was on to show the similarity between Information filtering and Information retrieval. Foltz and dumais researched tested methods for predicting which Technical Memos (TMs) best match people's technical interests. Within Bellcore, nearly 150 new TMs are published each month, yet very few are related to any single person's interests. Feedback using previous related abstracts provided an efficient and simple way of demonstrating people's interests [2]. This was totally based on previous feedback. There was no individual based filtering. In the trial filtering system being explored at Autodesk, a user chooses a discrete rating value (e.g., terrible, boring, somewhat interesting, no comment, very interesting) for each document read. A learning algorithm associates these user ratings with document features such as author, subject, selected keywords, organizations and shared ratings from earlier readers to prioritize incoming information [3].

This paper has addressed diversified domains including newswire articles, Internet "news" articles, and broader network resources. This paper focused on just prioritizing information by using rating values. The work by Boykin and Roychowdhury [4] that offers an automated anti-spam tool that, exploiting the properties of social networks, can recognize unsolicited commercial e-mail, spam and messages related with people the user knows. However, it is important to note that the strategy just stated does not exploit ML content-based techniques. J. Golbeck Offered an application, called FilmTrust, to personalize access to the website. But, such systems do not provide a filtering policy layer by which

the user can exploit the result of the classification process to decide how and to which extent filtering out unwanted information [5]. As far as privacy is concerned, current work is mainly focusing on privacy-preserving data mining skills, that is, protecting information related to the network, i.e., relationships/nodes, while performing social network analysis [6]. In microblogging services such as Twitter, there may arrive a situation where the users may become overwhelmed by the raw data. One solution to this problem is the classification of short text messages [7]. The proposed approach effectively classifies the text to a predefined set of generic classes such as News, Events, Opinions, Deals, and Private Messages. So, in this paper there was a focus on to classify news, opinions and other messages according to their categories.

### III. RELATED WORK

#### A. Existing System

We believe that this is a key OSN service that has not been provided so far. Indeed, today OSNs provide very little support to prevent unwanted messages on user walls. For example, Face book allows users to state who is allowed to insert messages in their walls (i.e., friends, friends of friends, or defined groups of friends). However, no content-based preferences are supported and therefore it is not possible to prevent undesired messages, such as political or vulgar ones, no matter of the user who posts them. Providing this service is not only a matter of using previously defined web content mining techniques for a different application, rather it requires to design ad-hoc classification strategies. This is because wall messages are Constituted by short text for which traditional classification Methods have serious limitations since short texts do not Provide sufficient word occurrences.

#### B. Proposed System

The aim of the present work is therefore to propose and experimentally evaluate an automated system, called Filtered Wall (FW), able to filter unwanted messages from OSN user walls. We exploit Machine Learning (ML) text categorization techniques [4] to automatically assign with each short text message a set of categories based on its content. The major efforts in building a robust short text classifier are concentrated in the extraction and selection of a set of characterizing and discriminate features. The solutions investigated in this paper are an extension of those adopted in a previous work by us from which we inherit the learning model and the elicitation procedure for generating pre-classified data. The original set of features, derived from endogenous properties of short texts, is enlarged here including exogenous knowledge related to the context from which the messages originate. As far as the learning model is concerned, we confirm in the current paper the use of neural learning which is today recognized as one of the most efficient solutions in text classification. In particular, we base the overall short text classification strategy on Radial Basis Function Networks (RBFN) for their proven capabilities in acting as soft classifiers, in managing noisy data and intrinsically vague classes. Moreover, the speed 2 in performing the learning phase creates the premise for an adequate use in OSN domains, as well as facilitates the experimental evaluation tasks.

### IV. IMPLEMENTATION

#### A. Filtering Rules

In defining the language for FRs specification, we consider three main issues that, in our opinion, should affect a message filtering decision. First of all, in OSNs like in everyday life, the same message may have different meanings and relevance based on who writes it. As a consequence, FRs should allow users to state constraints on message creators. Creators on which a FR applies can be selected on the basis of several different criteria; one of the most relevant is by imposing conditions on their profile's attributes. In such a way it is, for instance, possible to define rules applying only to young creators or to creators with a given religious/political view. Given the social network scenario, creators may also be identified by exploiting information on their social graph. This implies to state conditions on type, depth and trust values of the relationship(s) creators should be involved in order to apply them the specified rules. All these options are formalized by the notion of creator specification, defined as follows.

#### B. Online Setup Assistant for FRS Thresholds

As mentioned in the previous section, we address the problem of setting thresholds to filter rules, by conceiving and implementing within FW, an Online Setup Assistant (OSA) procedure. OSA presents the user with a set of messages selected from the dataset discussed in Section VI-A. For each message, the user tells the system the decision to accept or reject the message. The collection and processing of user decisions on an adequate set of messages distributed over all the classes allows to compute customized thresholds representing the user attitude in accepting or rejecting certain contents. Such messages are selected according to the following process. A certain amount of non neutral messages taken from a fraction of the dataset and not belonging to the training/test sets, are classified by the ML in order to have, for each message, the second level class membership values.

#### C. Blacklists

A further component of our system is a BL mechanism to avoid messages from undesired creators, independent from their contents. BLs is directly managed by the system, which should be able to determine who are the users to be inserted in the BL and decide when user's retention in the BL is finished. To enhance flexibility, such information are given to the system through a set of rules, hereafter called BL rules. Such rules are not defined by the SNM, therefore they are not meant as general high level directives to be applied to the whole community. Rather, we decide to let the users themselves, i.e., the wall's owners to specify BL rules regulating who has to be banned from their walls and for how long. Therefore, a user might be banned from a wall, by, at the same time, being able to post in other walls. Similar to FRs, our BL rules make the wall owner able to identify users to be blocked according to their profiles as well as their relationships in the OSN. Therefore, by means of a BL rule, wall owners are for example able to ban from their walls users they do not directly know (i.e., with which they have only indirect relationships), or users that are friend of a given person as they may have a bad opinion of this person.

## Extracting Messages from the Social Networks

This banning can be adopted for an undetermined time period or for a specific time window. Moreover, banning criteria may also take into account users' behavior in the OSN. More precisely, among possible information denoting users' bad behavior we have focused on two main measures. The first is related to the principle that if within a given time interval a user has been inserted into a BL for several times, say greater than a given threshold, he/she might deserve to stay in the BL for another while, as his/her behavior is not improved. This principle works for those users that have been already inserted in the considered BL at least one time. In contrast, to catch new bad behaviors, we use the Relative Frequency (RF) that let the system be able to detect those users whose messages continue to fail the FRs. The two measures can be computed either locally, that is, by considering only the messages and/or the BL of the user specifying the BL rule or globally, that is, by considering all OSN users walls and/or BLs.

## V. ARCHITECTURE

The conceptual architecture of OSN services is a three-tier structure (Figure1). The first layer is Social Network Manager (SNM), commonly aims to provide the basic OSN functionalities (i.e., profile and relationship management), however the second layer provides the support for external Social Network Applications (SNAs). The supported SNAs may in turn need an additional layer for their desired Graphical User Interfaces (GUIs). By considering this reference architecture, the proposed system is placed in the second and third layers. Users interact with the system by means of a GUI to set up and manage their FRs/BLs. Furthermore, the GUI provides users with a FW, that is, a wall where only messages that are authorized according to their FRs/BLs are published. The main components of the proposed system are the Content-Based Messages Filtering (CBMF) and the Short Text Classifier (STC) modules. STC goals to classify messages according to a set of categories.

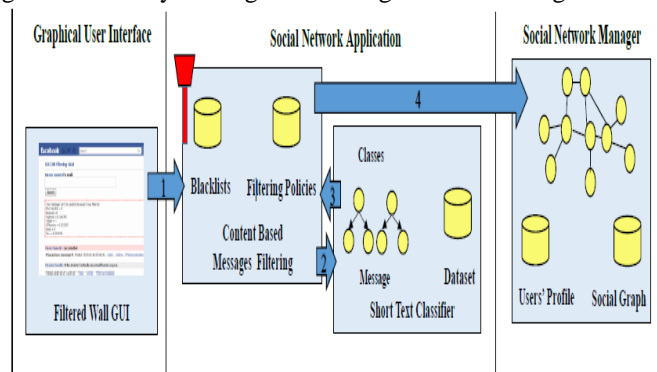


Fig.1. Filtered Wall Conceptual Architecture.

The first component exploits the message categorization provided by the STC module to enforce the FRs specified by the user. As shown in Fig.1, the path followed by a message, from its writing to the possible final publication can be given as follows:

- The user attempts to post a message after entering the private wall of his/her contacts which is interrupted by FW.
- A ML-based text classifier extracts metadata from the message content.

- Metadata together with data extracted from the social graph and users' profiles provided by the classifier is used by FW, to enforce the filtering and BL rules.
- The message will be published or filtered by FW Depending on the result of the previous step.

## VI. EXPERIMENTAL RESULT

Experimental results of this paper is shown in bellow Figs.2 to 4.

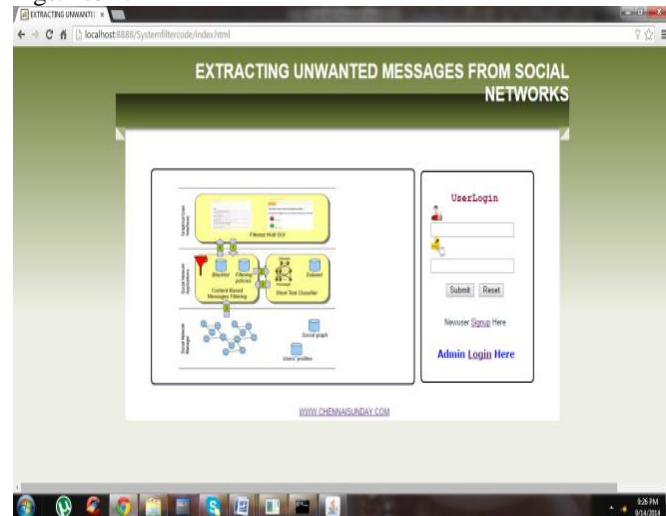


Fig.2. Main Form of the project.

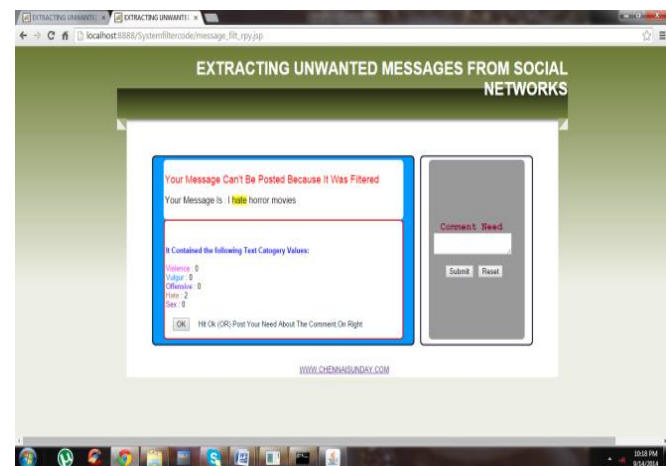


Fig.3. Filtering Walls.

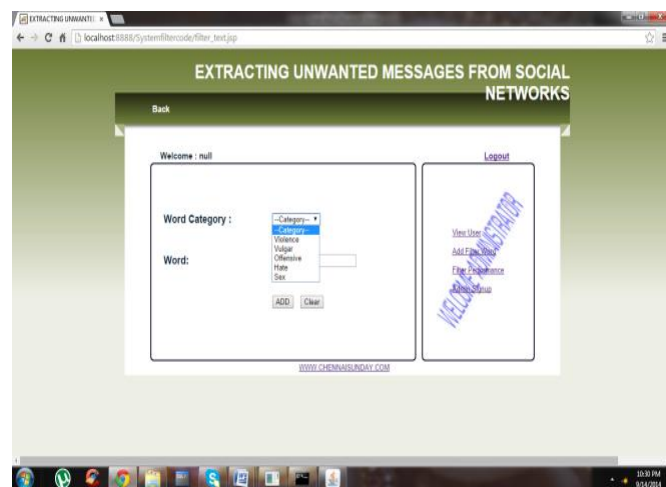


Fig.4. Adding Unwanted Messages.

## VII. CONCLUSION

In this paper, we have presented a system to filter unwanted messages from OSN walls. The system exploits a ML soft classifier to enforce customizable content-dependent FRs. Furthermore, the flexibility of the system in terms of filtering options is enhanced through the management of BLs. The first concerns the extraction and/or selection of contextual features that have been shown to have a high discriminative power. The second task includes the learning phase. As the underlying domain is dynamically changing, the collection of pre-classified data may not be representative in the longer term. The present batch learning strategy, based on the preliminary collection of the entire set of labeled data from experts, permitted an accurate experimental evaluation but needs to be developed to include new operational requirements. We plan to address this problem by investigating the use of on-line learning paradigms able to include label feedbacks from users in future work. The proposed system may suffer of problems similar to those encountered in the specification of OSN privacy settings. We plan to investigate the development of a GUI and a set of related tools to make easier BL and FR specification, as usability is a key requirement for such kind of applications.

## VIII. REFERENCES

- [1] N. J. Belkin and W. B. Croft, "Information filtering and information retrieval: Two sides of the same coin?" *Communications of the ACM*, vol. 35, no.12, pp. 29–38, 1992.
- [2] P. W. Foltz and S. T. Dumais, "Personalized information delivery: An analysis of information filtering methods," *Communications of the ACM*, vol. 35, no. 12, pp. 51–60, 1992.
- [3] P. E. Baclace, "Competitive agents for information filtering," *Communications of the ACM*, vol. 35, no. 12, p. 50, 1992.
- [4] Boykin, P.O., Roychowdhury, V.P.: Leveraging social networks to fight spam. *IEEE Computer Magazine* 38, 61–67 (2005).
- [5] J. Golbeck, "Combining provenance with trust in social networks for semantic web content filtering," in *Provenance and Annotation Data*, ser. *Lecture Notes in Computer Science*, L. Moreau and I. Foster, Eds. 2006
- [6] Carminati, B., Ferrari, E.: Access control and privacy in web-based social networks. *International Journal of Web Information Systems* 4, 395–415 (2008)
- [7] B. Sriram, D. Fuhry, E. Demir, H. Ferhatosmanoglu, and M. Demirbas, "Short text classification in twitter to improve information filtering," 2010P. J. Denning, "Electronic junk," *Communications of the ACM*, vol. 25, no. 3, pp. 163–165, 1982.
- [8] D. D. Lewis, Y. Yang, T. G. Rose, and F. Li, "Rcv1: A new benchmark collection for text categorization research," *Journal of Machine Learning Research*, 2004.
- [9] M. Vanetti, E. Binaghi, B. Carminati, M. Carullo, and E. Ferrari, "Content-based filtering in on-line social networks," in *Proceedings of ECML/PKDD Workshop on Privacy and Security issues in Data Mining and Machine Learning (PSDML 2010)*, 2010.

- [10] S. Pollock, "A rule-based message filtering system," *ACM Transactions on Office Information Systems*, vol. 6, no. 3, pp. 232–254, 1988.
- [11] Strater, K., RichterH.: Examining privacy and disclosure in a social networking community. In: *SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security*. pp. 157– 158. ACM, New York, NY, USA (2007).
- [12] F. Sebastiani, "Machine learning in automated text categorization," *ACM Computing Surveys*, vol. 34, no. 1, pp. 1–47, 2002.