ISSN 2349-9842, Volume 1, Issue 1, March 2014

INTERNATIONAL JOURNAL OF INNOVATIVE TRENDS AND EMERGING TECHNOLOGIES

AN EFFECTIVE SPAM FILTER USING BLOOM MECHANISM IN SOCIAL NETWORK

[1]Uma Maheswari.S, [2]Deepika.G,

[1]PG Scholar, Dept of CSE, Dhaanish Ahmed College of Engineering, Padappai, Chennai, Tamil Nadu, India
(E-mail: umapm3@gmail.com)
[2]Asst Prof, Dept of CSE, Dhaanish Ahmed College of Engineering, Padappai, Chennai, Tamil Nadu, India
(Email:deepi.g88@gmail.com)

Abstract-In Online Social Networks the internet mail server spam delivery is the most common issue. Email spam, also known as junk email or unsolicited bulk email (UBE), is a subset of electronic spam involving nearly identical messages sent to numerous recipients by email. In the Receiver Side only most of the modern spam-filtering techniques are deployed. They may be effective in selection junk mail for clients, but junk mail communications however preserve losing World-wide-web bandwidth along with the storage space of email hosting space. In existing system the Bayesian spam filters are easily poisoned by clever spammers who avoid spam keywords and add many harmless words in their emails. The detection system was proposed to monitor the simple mail transfer protocol (SMTP) sessions and email addresses in the outgoing mail messages from each individual internal host as the features for detecting spamming messages. Due to the huge number of email addresses observed in the SMTP sessions, Bloom filters are used to detect the spam messages and to increase efficiency.

Keywords: Spam filtering, Bloom filter, Short text classification.

1.INTRODUCTION

A social network is a social structure made up of a set of social actors (such as individuals or organizations). Most social network services are web-based and provide means for users to interact over the Internet, such as email and messaging. Web-based social networking services make it possible to connect people who share interests and activities across political, economic, and geographic borders. Some other social networks have further features, such as the ability to create groups that share common interests. Internet email is one of the most popular communication methods in our business and personal lives. Nowadays spam messages are becoming a continuous problem in email systems. Spam emails interfere with both email service providers and end users. Email spam, also known as junk email or unsolicited bulk email (UBE), is a subset of electronic spam involving nearly identical messages sent to various recipients by email. Blank spam may also occur when a spammer forgets or otherwise fails to add the payload when he or she sets up the spam run.

A spam filter should be personalized, and user-friendly. A more accurate filter generates less false positives and false negatives. False positives are legitimate emails that are mistakenly regarded as spam emails. False negatives are spam emails that are not detected. There are two primary types of spam filter attacks: poison attacks and impersonation attacks. In a poison attack, many legitimate words are added to spam emails, thus decreasing its probability of being detected as spam. In an impersonation attack, a spammer impersonates the identities of ordinary users by forging their IDs or compromising their computers. Spam filtering approaches can be mainly divided into two categories: content-based and identity-based. In the content-based category, emails are parsed and scored based on keywords and patterns that are typical in spam. The simplest identity-based spam filtering approaches are blacklist and white list, which check the email senders for spam detection. White lists and blacklists both maintain a list of addresses of people whose emails should not and should be blocked by the spam filter, respectively. One server-side solution records the number and frequency of the same email sent to multiple destinations from specific IP addresses. Identity-based spam filters identify spam based on the identities of email senders. Most modern spam-filtering solutions are deployed on the receiver side. These filters are good at filtering spam words for end users, but the spam messages are wasting Internet bandwidth and memory storage.

To detect spamming bots, use the detection system to monitor the SMTP sessions and track the number and the uniqueness of the recipients email addresses in the outgoing mail messages from each individual internal host as the features for detecting spamming bots. Due to the huge number connected with email deals with affecting the SMTP periods, shop the deals with along with deal with these people effectively inside the Bloom filters. One fundamental issue in today's Online 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. This is achieved through a flexible rule-based system that allows users to customize the filtering criteria to be applied to their walls. The automated system, called Filtered Wall (FW), able to filter unwanted messages from Online Social Network (OSN) user walls.

2. RELATED WORK

In 2005 S. J. Delany and P. Cunningham had discussed about the spam filtering system that uses machine learning will need to be dynamic. Case-Based Reasoning (CBR) is a lazy approach to machine learning where it is delayed to run time. In this paper the detailed description of such a system called evaluate design decisions concerning the case representation. It compares the performance with an alternative system that uses Naive Bayes. The initial stage of this research focused on identifying the most appropriate case base configuration for a case-based classifier for spam filtering. CBR as a lazy learner offers significant advantages; it provides capabilities to learn without the need for a separate learning process and facilitates extending the learning process over different levels of learning.

In 2006 H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman had discussed about the sybil attack, a malicious user can create multiple fake identities and pretends to be multiple, distinct nodes in the system. This paper presented Sybil Guard, a novel decentralized protocol for limiting the corruptive influences of sybil attacks, by bounding both the number and size of sybil groups. Sybil Guard relies on properties of the users' underlying social network, namely that (i) the honest region of the network is fast mixing, and (ii) malicious users may create many nodes but relatively few attack edges.

In 2007 P. Haider, U. Brefeld, and T. Scheffer had proposed the problem of detecting batches of emails that have been created according to filter spam more effectively by exploiting collective information about entire batches of jointly generated messages. A sequential decoding procedure and it derives the corresponding optimization problem of supervised clustering. A sequential clustering algorithm and two integrated formulations for learning a similarity measure to be used with correlation clustering.

Using the batch information the email spam classification performance increases largely the information. The efficiency of the clustering algorithm makes supervised batch detection in enterprise-level scales, with millions of emails per hour and thousands of recent emails as feasible.

The problem of filtering spam messages for many users is each user receives messages according to an individual or unknown. A hierarchical Bayesian model also generalizes across users by learning a common prior which is imposed on new email accounts. It improves the performance of a personalized spam filter provided that the inbox contains sufficiently many messages. The Dirichlet-enhanced bias correction method estimates and compensates for the discrepancy between labeled training and unlabeled personal messages, learning from the new user's unlabeled inbox as well as from data of other users.

3. PROPOSED SYSTEM

In proposed system the spam filtering techniques are going to deploy on the sender side itself. By this the spam message cannot send to the receiver side. Spam email may also include malware as scripts or other executable file attachments. Before sending the mail it can able to filter the spam, normally some files come with an extension of .exe and encrypted file sent to the mails. Using filtering technique the junk mail can neglect the encrypted spam too. This system will improve bandwidth and memory storage. There are two techniques which is used to find the encrypted format text, Word Net dictionary and short message technique. The Bloom filters are used to find the junk mail, it have an advantage on other data structures for representing sets, such as self balancing binary search tree. This prevents text based spam filters from detecting and blocking spam messages. And it is used to improve the performance of Online Social Network. This system used to reduce the

In previous system spam mails are filtering on the receiver side. The sender mail before filtering, so spamming activities still exist, and spam messages still waste Internet bandwidth and the storage space of mail servers. Spamming bots may access web mail interfaces or deliver via secure SMTP for spamming. Since the packets are encrypted, the detection method cannot identify the spamming bots in this system. Bayesian spam filters need a considerable amount of time to adapt to a new spam based on user feedback. A Bayesian filter has a list of keywords along with their probabilities to identify an email as a spam email or a legitimate email. The spamming bot should deliver spam messages to a wide range of unique REAs for efficient spam delivery.

Since social networks have many unwanted messages that used to be displayed on wall so that the memory space is wasted.

Content-based Approaches

The basic approach of content-based spam filtering is the static keyword list, which however makes it easy for a spammer to avoid filtering by tuning the message. The second category of content-based approaches includes machine learning based approaches such as Bayesian filters, decision trees, Vector Machines, Bayes Classifiers and combinations of these techniques. In this approach, a learning algorithm is used to find the characteristics of the spam and of legitimate emails. Then, future messages can be automatically categorized as highly likely to be spam, highly likely to be legitimate emails, or somewhere in between. The third category of content-based approaches is collaborative spam filtering. Once a spam email is detected by one user, other users can avoid the spam later on by querying others to see if their received emails are spam or not.

Identity-based Approaches

Identity-based spam filters identify spam based on the identities of email senders. The simplest identity-based spam filtering approaches are blacklist and whitelist , which check the email senders for spam detection. Both Whitelists and blacklists maintain a list of addresses of people whose emails should not and should be blocked by the spam filter, respectively. The server-side records the number and frequency of the same email sent to multiple destinations from specific IP addresses. If the number of spam mails increases, the node with the specific IP address is blocked and the people cannot use the email account again.

A Bayesian filter has a list of keywords along with their probabilities to identify an email as a spam email or a legitimate email. It used to identify an email as spam depending on the probability based on user. The user can identify an email as junk mail or not.

3.1 Social Closeness-based Spam Filtering.

When a person receives an email from another socially close person, the email has a low probability of being spam unless the email sender's machine is under an impersonation attack. Thus, the social closeness between individuals can be utilized to improve the accuracy of spam detection. Note that, in a social network, people treat others differently based on their social closeness. People impose different levels of interest, trust, or tolerance to the emails from others with different social closeness. People with close social relationship are willing to receive emails from each other. The emails containing spam keywords from senders that are socially far away.

CLOSENESS ALGORITHM.

1: Send a query message with TTL
2: **if** Receive a response from destinations **then**
3: Calculate its closeness with each node using Equ.
4: **end if**
5: **if** Receive a query initiated by node i**then**
6: Insert its closeness with node ito the message
7: TTL=TTL-1
8: **if** TTL¿0 **then**
9: Forward the message to its neighbors
10: **else**
11: Send the message to node i
12: **end if**
13: **end if**

It regards the spam as emails that receivers are not interested in. Therefore, it needs to differentiate emails from persons with different social closeness. SOAP loosely checks emails between individuals with high closeness and strictly checks emails between individuals with low closeness. The social closeness-based spam filtering module checks emails based on the closeness between the receiver and the sender. A smaller closeness rate leads to stricter checking, while a larger closeness rate leads to looser checking.

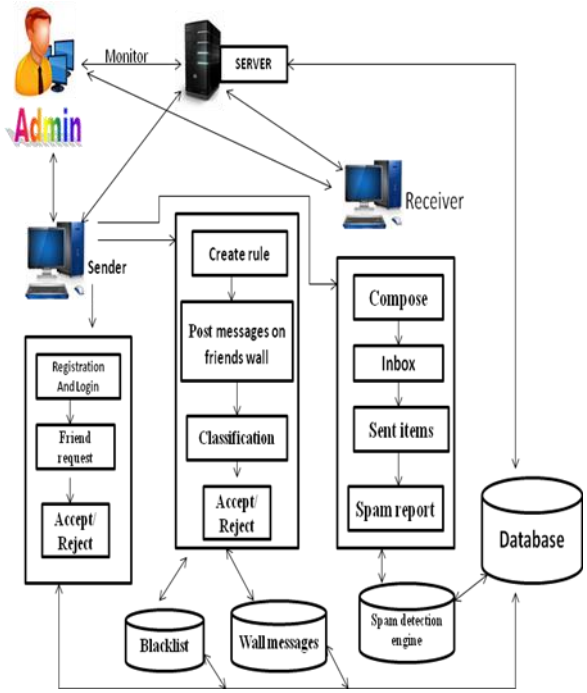

Fig 1 workflow of spam filtering

3.2 Bloom filter

A Bloom filter is a data structure optimized for fast and space-efficient. Bloom filters have a strong

space advantage over other data structures for representing sets, such as self balancing binary search tree. Stable Bloom filters as a variant of Bloom filters for streaming data. Stable Bloom filters continuously remove old information to make room for more recent elements. Since old information is ejected, the Stable Bloom filter introduces false negatives, which do not appear in fixed bloom filters. It shows that a tight upper bound of false positive rates are guaranteed, and the method is better to standard bloom filters in terms of false positive rates and time efficiency when a small space and an acceptable false positive rate are given. Bloom filters that can adjust dynamically to the number of nodes stored, while assuring a minimum false positive possibility rate. This technique is based on sequences of standard bloom filters with increasing ability and false positive probabilities, so as to make sure that a maximum false positive probability can be set earlier, regardless of the number of elements to be inserted.

3.3 Filtering rules

The Content-Based Messages Filtering (CBMF) and the Short Text Classifier methods are used in filtering rules. With Online networks a similar communication might have various meanings along with relevance according to whom creates the idea. The actual significant work in building a strong short text classifier (STC) are targeted in the removal in addition to offering of a new pair of characterizing in addition to attributes. Information filtering can consequently be used to give users the facility to automatically organize the messages written on their own walls, by filtering out unwanted messages. Black List mechanism is used to avoid messages from undesired creators. Black Lists are directly managed by the system, which should be able to conclude who are the users to be inserted in the BL and decide when users maintenance in the BL is finished. To improve flexibility, such information are given to the system and a set of rules, are called BL rules.

3.4 Detection Accuracy

The accuracy rate as the ratio between the number of successfully classified emails and the number of all received emails. The interest-based spam filtering component increases the spam detection accuracy by filtering out the emails in the receiver's disinterests and accepting the emails that match the receiver's interests.

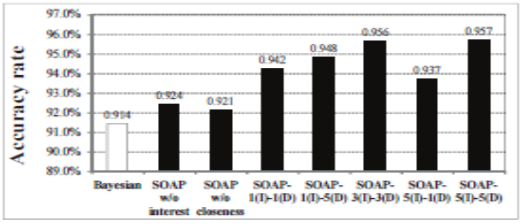

Fig 2 Accuracy

A node can send a spam message to more friends in its social network as the nodes in RE within the same social network are likely to trust each other when the spammer sends the spam into the social network. A more accurate filter generates less false positives and false negatives. False positives are legitimate emails that are incorrectly regarded as spam emails. False negatives are spam emails that are not detected.

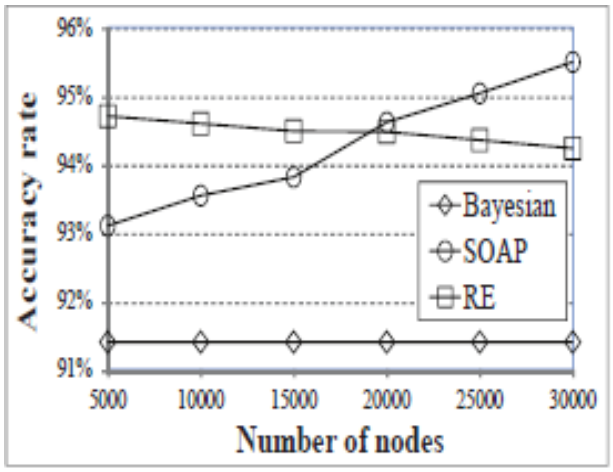

Fig 3 Accuracy vs. network size

There are two primary types of spam filter attacks: poison attacks and impersonation attacks. In a poison attack, many legitimate words are added to spam emails, thus decreasing its probability of being detected as spam. In an impersonation attack, a spammer impersonates the identities of ordinary users by forging their IDs or compromising their computers. In contrast, Bayesian completely relies on data training and needs a significant amount of data and time to learn a new spam keyword.

The false negative (FN) rate is the number of false negatives divided by the total number of emails, and the false positive (FP) rate is the number of false positives divided the total number of emails.

4. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

The performance of SOAP with bloom filter is used to analyze the false positive and false negative. The false negative (FN) rate is the number of false negatives divided by the total number of emails, and the false positive (FP) rate is the number of false positives divided by the total number of emails.

The False Negative rate of Bloom filter decreases as the sample size since more samples enable filter to learn more about the users and personal preferences. In SOAP, some emails that disinterest a receiver can be determined directly from the personal profile without training, thus the False Negative rate does not greatly vary as the sample size increases .Bloom component can learn those (dis)interest keywords, which enable SOAP to detect the spam that cannot be identified by the (dis)interest keywords checked by the poorly trained Bloom component.

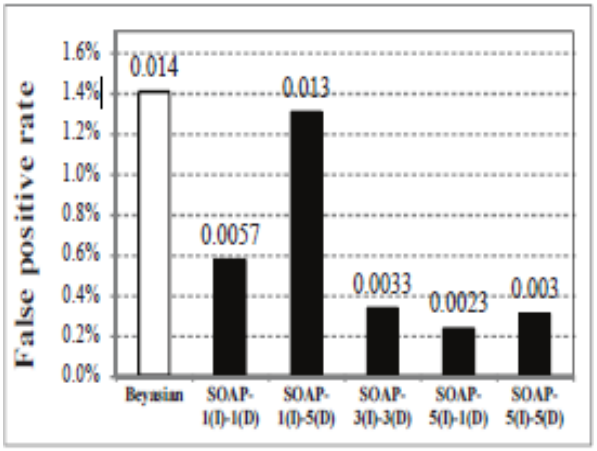

Fig 4 False positive rate

5. CONCLUSION

In this paper, a SOcial network Aided Personalized and effective spam filter (SOAP) is proposed to meet the problem. In SOAP, nodes form a network for connecting the social friends. Each node uses SOAP to prevent spam separately. SOAP integrates a new component such as Bloom filter. The social closeness-based spam component prevents spam poison attacks, the social interest-based spam component helps to realize personalized spam filtering, the adaptive trust management component prevents impersonation attacks, and the friend notification scheme improves the power of a collective of socially close nodes to strengthen SOAP's ability to answer the impersonation attacks. Accurate spam filtering results function as input for Bloom filter used to have automatic training with reduced user effort to divide spam emails. The results of prototype based experiments show that SOAP improves on the performance of the basic Bloom filter in term of spam detection accuracy and training time. The filtering rules that created to block the unwanted messages can be filtered by user that posted on user wall. In future the performance and security of the social network can be improved by SOAP.

REFERENCES

1. P. Haider, U. Brefeld, and T. Scheffer. Supervised Clustering of Streaming Data for Email Batch Detection. In Proc. of ICML, 2007
2. S. Bickel and T. Scheffer. Dirichlet-enhanced Spam Filtering based on Biased Samples. In Proc. of NIPS, 2007
3. S. J. Delany and P. Cunningham. An Assessment of Case-based Reasoning for Spam Filtering. Artifical intelligent review, 2005
4. F. Fdez-Riverola, E. Iglesias, F. Diaz, J. R. Mendez, and J. M. Corchado. Spam Hunting: An Instance-based Reasoning System for Spam Labeling and Filtering. Decision Support System, 2007
5. W. Zhao and Z. Zhang. Email Classification Model based on Rough Set Theory. In Proc. of AMT, 2005
6. F. Zhou, L. ZHuang, B. Y. Zhao, L. Huang, A. D. Joseph, and J. D. Kubiatowicz. Approximate Object Location and Spam Filtering on Peer-to-Peer Systems. In Proc. of Middleware, 2003
7. O. Boykin and V. Roychowdhury. Personal Email Networks: An Effective Anti-spam Tool. IEEE Computer, 2004
8. H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman. SybilGuard: Defending against sybil attacks via social networks. In Proc. Of SIGCOMM, 2006.