IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XI (Mar-Apr. 2014), PP 19-22
www.iosrjournals.org

Secured Tagging [Redefining Spam Detection]

S.Himaja[1,] Dr.N. Chandra Sekhar Reddy[2,] S.Srinivas[3]

[1] *Student, M.Tech IT Dept., Institute of Aeronautical Engineering, HYD-500043, AP, India.*
[2] *Professor, CSE Dept., Institute of Aeronautical Engineering, HYD-500043, AP, India.*
[3] *Asst.Professor, IT Dept., Institute of Aeronautical Engineering, HYD-500043, AP, India.*

Abstract: *Recently Social bookmarking websites have emerged for finding and promoting relevant websites among its users. People can add bookmarks to promote the links and have a total control over their bookmarks. Because of the multimedia contents social networking sites became so popular around the web. However spam is the one thing that is still annoying the users to perform productive searches. Spam tags that are totally irrelevant to these content enriched sites appear malicious in general. There are various techniques used to control such tag spam. We discussed one of those techniques in this paper, Trust modeling approaches can be classified into 2 categories according to the target of trust, i.e., user and content trust modeling to predict spam, the spam factor(P) is calculated and basing on its value P is categorized into one among High (H), Low (L) and Medium (M) levels.*

Keywords: *Spam detection, Social Bookmarking, tags, spam factor*

I. Introduction:

Social systems enable users to store, share, and search and consume content online. Tagging in social systems has become progressively widespread since the transition to net 2.0, because it simplexes and eases search and retrieval of data. While interacting with each other, users are permitted to access these data globally. Tags may be allotted to different styles of resources like pictures, videos, publications and bookmarks, creating it a valuable plus to look engines on web and in social tagging systems. Users could build mistakes in tagging and resources could also be maliciously superimposed for advert. As it becomes long if filtering spam annotations and spammers is done manually, we utilize machine learning approaches to facilitate this method. We can classify progressive approaches to get rid of spam in social tagging into many classes and put them together to compare and distinct them for further analysis to give a better user experience.

II. Existing System

With Internet becoming a majority source people to find and gather online information, spam tagging has become an easy way for spammers to make use of it to their own profit. Before the Internet boom, social tagging and spam content was used to occur only in emails and few varied domains. But today even the information friendly blogs are also being spammed just to build back links and increase traffic to their websites. So many popular websites like Amazon, eBay etc are bound to attract spam in social tagging because of their usage. [1]

Many filtering techniques to exclude biased ratings are planned inside the literature. Sadly, the countermeasures developed for website spam and e-mails don't directly apply to the social networks that we use.

III. Proposed System:

There are 3 levels where the spam can be inserted into social tagging system namely spammer, spam content and spam tag content association. At each and every of these levels, trust modeling is performed to prevent the spam tags in a much better way. Trust modeling approach can be divided into two categories depending upon the target of trust. The spam factor in social tagging system is calculated in 3 levels High (H), Medium (M) and Low (L).

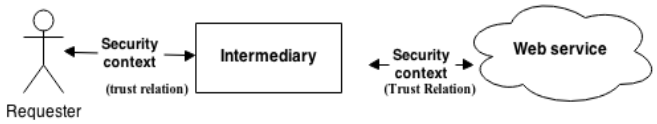
If the outcome of the spam is H (High) or M (Medium) then the message is treated as spam. If it displays the messages as L (Low), it won't be treated as spam.

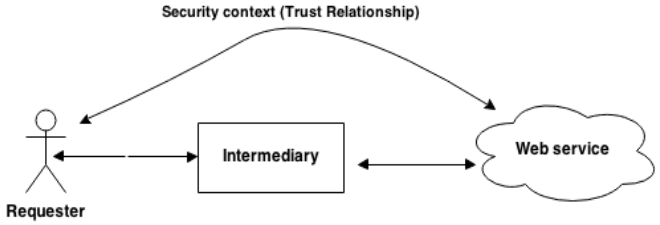
Modules:

I. ***Content Trust Modeling***
II. ***User Trust Modeling***
   i. ***Centralized User Trust Modeling***
   ii. ***Distributed User Trust Modeling***

1. Content Trust Modeling:

It is used to categorize content such as videos, web pages as licit or spam. Here, content is the target of trust, and hence based on its content and (/or) associated tags a trust score is given to each content [1].





2. User Trust Modeling:

Basing on the data derived from a user's account, every user is given a trust score and basing on this score that particular user might be flagged as licit user or illegitimate user. User trust can be built in either centralized or distributed manner. [2]

i. **Centralized User Trust Modeling:**

Here one central authority (manager) maintains all trust models .These are used in social networks (e.g.[3], [4], [5])

ii. **Distributed User Trust Modeling:**

Basing on the previous interactions with other users, each user maintains their own manager. These are mainly used in P2P networks. [2]

Algorithm

This is the formula referenced by Paul Graham in his 2002 article;this formula is sometimes called as a naive Bayes classifier. Bayesian spam filtering algorithms [6] are rooted on formulas that are precisely valid only if the terms existing in the message are independent events. This condition is not generally satisfied (e.g., in natural languages like English, the chance of finding an adjective, as an example, is affected by the probability of getting a noun.), however it is a useful glorification, specially since the statistical correlations between individual words are normallyunknown. Basing on this, one can derive the following formula from Bayes' theorem: [7]

$$p = \frac{p_1 p_2 \cdots p_N}{p_1 p_2 \cdots p_N + (1-p_1)(1-p_2)\cdots(1-p_N)}$$

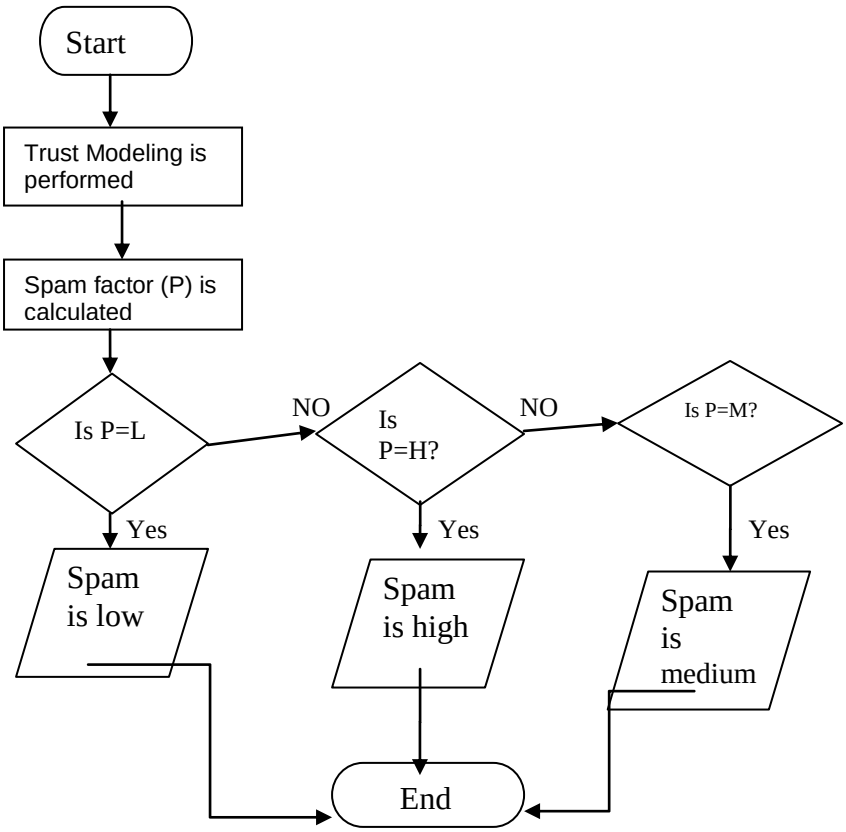
Where:

- P is the probability that the tag suspected is spam.
- P1is the probability P (S|W1) that it is a spam knowing it consists of a first word (e.g. "copy");
- P2is the probability P (S|W2) that it is a spam knowing it consists of a secondary word (e.g. "fire");
- PN is the probability P (S|WN) that it is a spam knowing it consists of an associate ordinal word (e.g. "rings").

The result P is typically compared to values as shown in table to define the level of spam which is categorised into 3 levels.

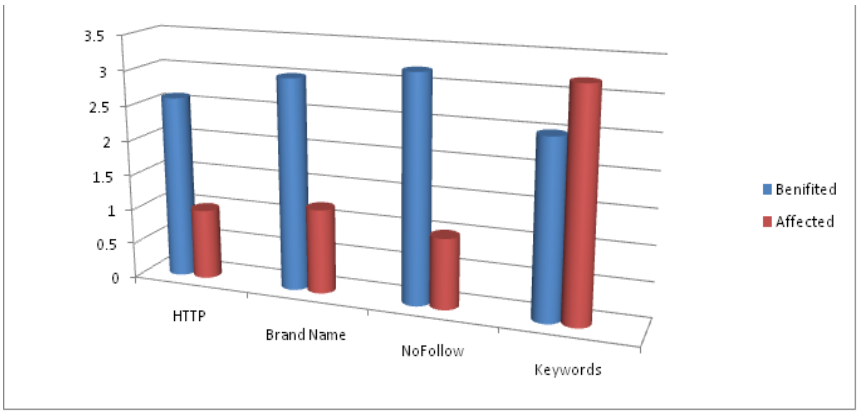
1. Low (**L**)
2. Medium (**M**)
3. High(**H**)

P value	Content-level
0.0-0.2	Low(L)
0.2-0.6	Medium(M)
0.6-1.0	High(H)



IV. Result

The Resultant Graph after implementation of Anti-Spam algorithms would be like this:



V. Conclusion And Future Research

Here, we cope with one amongst the key issues in tagging systems: combating noise and spam and classify existing studies among the literature into two categories, i.e., content and user trust modeling. Representative techniques in each category were analyzed and compared.

Additionally we formulate spam factor and determine the level of spam in specific content. Further, one can use additional security mechanisms if spam content is high.

References

[1] http://infoscience.epfl.ch/record/167698/files/Ivanov_201202_IEEESPM2012.pdf
[2] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systemsfor online service provision," Decision Support Syst., vol. 43, no. 2, pp. 618–644,Mar. 2007.
[3] B. Markines, C. Cattuto, and F. Menczer, "Social spam detection," in Proc.ACMAIRWeb, Apr. 2009, pp. 41–48.
[4] I. Ivanov, P. Vajda , J.-S. Lee, L. Goldmann, and T. Ebrahimi, "Geotagpropagation n social networks based on user trust model," Multimedia Tools Applicat., pp.1–23, July 2010.
[5] F. Benevenuto, T. R odrigues, V. Almeida, J. Almeida, and M. Gonçalves,"Detecting spammers and content promoters in online video social networks," inProc. ACM SIGIR, July 2009, pp. 620–627.
[6] http://en.wikipedia.org/wiki/Bayes%27_theorem#Extended_formhttp://www.mathpages.com/home/kmath267.htm