International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:9, No:1, 2015

Facebook Spam and Spam Filter Using Artificial Neural Networks

Fahim A., Mutahira N. Naseem

***Abstract*—**Spam is any unwanted electronic message or material in any form posted too many people. As the world is growing as global world, social networking sites play an important role in making world global providing people from different parts of the world a platform to meet and express their views. Among different social networking sites Facebook become the leading one. With increase in usage different users start abusive use of Facebook by posting or creating ways to post spam. This paper highlights the potential spam types nowadays Facebook users' faces. This paper also provide the reason how user become victim to spam attack. A methodology is proposed in the end discusses how to handle different types of spam.

***Keywords*—**Artificial neural networks, Facebook spam, social networking sites, spam filter.

I. Introduction

SOCIAL networks are one of the most popular and easiest forms of communication. They enable its users to communicate, share and distribute a significant quantity of information. They depict the social image of a person. Daily and continuous communications results in exchange of content as messages, images, and pictures, audio and video data. These sharing and social networking relations make ones presence more valuable. The world of Facebook and other social networking sites provide users a feeling to be in an "avatar" where they do anything from meeting friends to playing games and much more. This takes person into its charisma that no one willing to leave this world.

According Facebook statistical studies, per month average user creates 90 contents (messages, videos, pictures etc) and per annul over 30 million such contents are being created. When such huge amount of data is creating making user careless with whom to share data or which apps are worthy of using and which make abusive use of your information.

Facebook is leading social networking site having user more than 1 billion. As with such huge amount of users many risks are also associated with it. These users willingly or unwillingly provide a lot of information and data so that it becomes sometimes difficult to decide relevant and useful content and other spams.

SPAM is defined as unwanted electronic messages [1] posted blindly too many number of recipients [2]. In Facebook, spam may of different types based on who posted and the location where posted.

Facebook provides users a feature who is allowed to post on one's wall and who's not. But most of the time it is observed that many unwanted data in the form advertisements by pages, vulgar contents, dubious products, get-rich schemes etc.

In this paper, Facebook spams are discussed and how they affect users. Spam filter allow information to filter out unwanted message from the newsfeed. This paper will discussed different spam filtering techniques proposed for Facebook and how spammers able to keep posting spam using different means. In the end of this paper spam filtering model will be presented using artificial networks to block potential spams.

This paper is organized as follows: I) Introduction, II) related work, III) Types of Facebook Spam IV) Link between Spam Types and Spam Victims V) Proposed Methodology: Spam Filtering Model using Artificial Neural Network VI) Advantages and Disadvantages VII) Conclusion.

II. Related Work

Tak et al. present a novel method for mail spam detection [3]. In this paper they present a spam detection technique based on query generation with the help of knowledge base and artificial neural networks. This approach detects email spam based on mail behaviors, mail header analysis and cross validation. Proposed methodology suggests 7 steps to analyze the incoming mail decide and take action accordingly. Their results show 98.17% spam filtered out and 0.12% false alarm. This paper has some limitations as needs more hardware for the execution and higher memory space.

Ho et.al studies the privacy protection issues in social networking sites (SNS) [4]. There are many potential threats as identity theft and disclosure of sensitive and personal information. Many users are not aware of these threats and related privacy settings. Privacy settings provided by SNS are not flexible enough to shield user information and data. This paper conducts a survey to highlight issues related to safety and privacy in social sites.

Ariaeinejad et al. proposed a spam detection technique based on Interval Type-2 Fuzzy Set [5]. The results obtain shows that its effective technique in detecting spam and email categorization. The proposed technique enable users to have control over different categories of spam and personalization of the spam filter.

Markov Clustering (MCL) based approach is presented for detecting profile spam in online social networks [6]. This approach uses the real dataset of Facebook profiles. This

F. Arif is with the National University of Sciences and Technology (NUST), Islamabad, Pakistan (phone: 0092-51-9272102; e-mail: fahim@mcs.edu.pk).

M. N. Tahir is with the Computer Software Engineering Department, National University of Sciences and Technology, Islamabad, Pakistan (e-mail: mutahiranaseem.mscs19@students.mcs.edu.pk).

technique filters out spam in the form of friends, page likes and URL's shared.

Dhanaraj et al. present an overview of existing image-spam email filtering techniques along the concept of spam emails [7]. This paper discusses various solutions proposed by different researchers. The main concern is design a technique to reach an ideal case i.e. to eliminate 100% spam. This paper reviewed spam techniques based on the relative cost of two types of errors as ham/spam recall and ham/spam precision.

Nosseir et al. present an approach based on intelligent word base spam filter using mutli-neural networking [8]. Each neural network is trained based on a normalized weight from the ASCII value of the word character. Based on the character weighted value words are characterized as bad or good. The results show high false positive and low false negative percentage.

Kumar et al. discuss the privacy and security concerns, attacks and their respective prevention techniques in social networking sites [9]. This research paper suggests that proper knowledge of the hacking strategies will provide best defense against cyber-attacks. They propose architecture for secure request response exchange of data users.

Vanetti et al. present approach to control messages posted on the wall to avoid that unwanted content is displayed [10]. This approach provides online social networking users direct power to manage messages being posted on their walls. This is achieved through a flexible rule-based system that allows customizing the filtering criteria.

III. Types of Facebook Spam

Facebook spammers devised different types of spam. Most common of these spam types are discussed below;

A. Facebook Link Spam

Most of the time it is observed that short links referring to videos of famous celebrities.

B. Application Request Spam

Sometimes application request lead users to install a Facebook that requires a user authorize the ability to posts to walls and friend pages.

C. Message Spam

Facebook introduces feature that allows sending message to anyone even who is not in friend list. This creates an issue of bulk of spam messages.

D. Share-to-Win Images/Videos

This spam type asks victims to share image or like page in return get some prize (win i-pads or lottery tickets).

E. Click-Jacking or Like-Jacking

On Facebook sometimes one sees his friend like something that seems questionable. This spam work as one sees as some friend posted a video or some other link. When this link is clicked asked for online survey and sharing of personal information or signing up for products etc. Code is embedded in links used that spread to her own page making it seem as she liked it [11].

F. Facebook Subscribe

This feature allows anyone else public posts even two are not friends. Many public figures have open profiles for subscribers to see their posts. This feature leads spam from thousands of users around the world posted.

G. Snoop Spam

Images and posts are virally shared that sound too good to be true. These work as game "telephone", sometimes may be true as some point but regular sharing and messages totally alter the meanings. These may include Bill Gates gives up his wealth or Facebook announces to close account etc.

H. Comment Spam

There is a lot of comments spam appearing in the comments. These are mostly product advertisements like Dr. Oz product. These advertisements when clinked may hijack the account or may contain viruses and malwares.

IV. Link between Spam Types and Spam Victim

Users have different preferences about friends they usually interact with on Facebook. Friends mostly open or view videos shared by friends they knew well [12]. In this paper these friends are categorized on the basis of how frequently they interact with them or trust level.

A. Casual Friend

User knew friend only through Facebook or online source.

B. Best Friend

Friends with whom user interact frequently as commenting on their walls, images, videos etc.

C. Normal Friends

User interacts with these friends from time to time. They include family members and friends from work place, school, and college and from real life.

D. Visitors

They usually follow someone or like pages

TABLE I
Trend of How User Becomes Spam Victim

	Casual friends	Best friend	Normal friends	Visitors/ page likes
Facebook link spam	low	high	High	low
Application request spam	Low	high	medium	low
Share-to-win images/videos	medium	high	medium	Low
Message spam	medium	low	Low	high
Click jacking or like jacking	medium	high	medium	low
Facebook subscribe	low	low	Low	high
Snoop snap	medium	high	High	low
Comment spam	medium	low	medium	high

Table I shows the trust level of person when user becomes a victim of spam. If user knows a person who posted spam then

it's more likely to accept his/her different application requests. The table shows the trend that if something is posted by close/best friend users usually goes to open them or likes them. In doing so sometimes may become victim spam attack.

V. Methodology

Facebook spam filtering using Artificial Neural Networking: the proposed methodology works using the given following steps.

A. Analyze the Post Content

Firstly analyze the posted wall contents. If the pattern of the wall post did not match the pattern of the friend's wall post pattern then mark as "spam".

B. Trusted Knowledge Base

Knowledge base is a good, efficient and effective way to give results based on historical data. In this section friends' data and their pattern of wall posts are stored. In the trusted knowledge base, database of friends' activity is saved based on frequency of friends' activity. This knowledge base is responsible for detecting the suspicious spam activity from the friend list.

C. Spam Knowledge Base

A knowledge base would be maintained at the back end. This knowledge base contains keywords based on the type of possible Facebook spam. During this step categories of Facebook spam are defined according to their categories. When spam categories are defined keywords associated with each spam type is also defined based on good/ bad words. In bad word directory sex, win-a-prize, app request etc. are included.

D. Misbehavior of Posts

Misbehavior is executing using Artificial Neural Network. Artificial Neural Network used to that allows system to adopt behavior based on their data. In this spam filtering model, ANN learns the complex and varying behavior of Facebook spam and makes intelligent and efficient decision based on the posted friends' activity.

E. Validation

During this step system already detects the spam in any form and stops it to appear in the one wall. Decision about the suspected spam is made.

VI. Advantages And Disadvantages

The proposed solution handles different Facebook spams. But the proposed solution has some plus and weak points also as described below:

A. Advantage

1. The proposed method will detect spam posted by person present in friend list
2. This system observes the pattern of the activities of friends and their frequency of doing activities.

B. Disadvantage

1. The proposed solution does not support the Facebook subscribe feature spam.

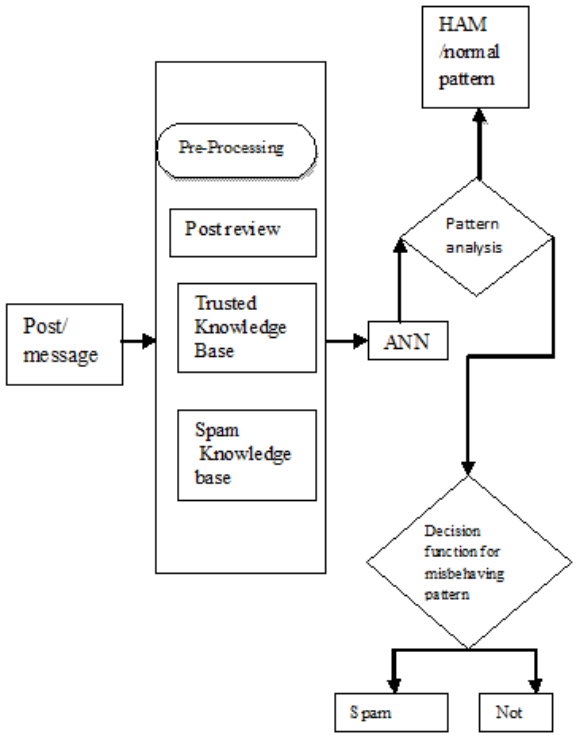

Fig. 1 Proposed Model

VII. Conclusion

Facebook is world most using social networking site. Day by day number of Facebook users' increases, their purpose to use it also changes with time. Now a day's people use Facebook to run their business, advertise their products but apart from this healthy use sometimes users use it to annoy other. This paper covers the means users or we may call them spammers misuse Facebook. Some users intentionally and some unintentionally post spam over Facebook. In the end methodology is proposed which uses the knowledge of artificial neural networks to study normal the behavior of friend list and detect unusual behavior resulting in spam. Pons and cons of this proposed methodology is also listed. Facebook spams are new area that needs researchers to do work. In the future this methodology needs to be implemented to verified that the results of this methodology.

References

[1] V.N. Vapnik, H. Druck, D. Wu, "Support Vector Machines for Spam Categorization", IEEE Transactions On Neural Networks, vol. 10 no.5 , pp. 1048-1054, Sep 1999.

[2] L. Lazzari, M. Mari, A. Poggi, "A collaborative and multi agent approach to e-mail filtering", IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT'05), pp. 238-241, 2005

[3] G. K. Tak and S. Tapaswi "Query based approach towards spam attacks using artificial neural network" International Journal of Artificial

Intelligence & Applications (IJAIA), vol.1, no.4, October 2010 DOI : 10.5121/ijaia.2010.1407 82
[4] A. Ho, A. Maiga and E. Aïmeur "Privacy Protection Issues in Social Networking Sites" IEEE, 2009
[5] Reza Ariaeinejad and AlirezaSadeghian "Spam Detection System: A New Approach Based on Interval Type-2 Fuzzy Sets" IEEE CCECE , Canada,2011
[6] F. Ahmed and M. Abulaish "An MCL-Based pproach for Spam Profile Detection in Online Social Networks"IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications 2012
[7] S. Dhanaraj and Dr. V. Karthikeyani "A Study on E-mail Image Spam Filtering Techniques" Proceedings of the 2013 International Conference on Pattern Recognition, nformatics and Mobile Engineering (PRIME), pp. 21-22,February 2013.
[8] A. Nosseir, K. Nagati and I. Taj-Eddin "Intelligent Word-Based Spam Filter Detection Using Multi-Neural Networks" IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 1, March 2013M. Young, *The Techincal Writers Handbook*.Mill Valley, CA: University Science, 1989.
[9] A. Kumar, S. K. Gupta, A. K. Rai and S. Sinha "Social Networking Sites and Their Security Issues" International Journal of Scientific and Research Publications, vol. 3, no 4, April 2013
[10] M. Vanetti, E. Binaghi, E. Ferrari, B. Carminati, and M. Carullo "A System to Filter Unwanted Messages from OSN User Walls" IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 2, february 2013
[11] DolvaraGunatilaka "A Survey of Privacy and Security Issues in Social Networks"www.cse.wustl.edu/~jain/cse571-11/ftp/social/
[12] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: automated identity theft attacks on social networks," in Proceedings of the 18th International Conference on World Wide Web(WWW'09). ACM, pp. 551–560, 2009

Dr. FahimArif has done Bachelors in Telecommunication from College of Telecommunication Engineering (UET Lahore) in 1995 and Master in Sciences in Computer Software Engineering from National University Science and Technology, Islamabad in 2003. He has won NUST Endowment fund scheme scholarship for NUST in 2003 and International Research Support Initiative Program Fund from HEC in 2007. He has completed his PhD degree from National University Science and Technology in 2009.

His contribution to international research in recent few years is excellent. He has presented/published numerous research papers in different international conferences including USA and Canada. In addition to his research publications, he is doing as reviewer for various international conferences. He worked as international research scholar in System and Computer Engineering Department, Carleton University, Ottawa, Canada in 2007 and participated in numerous research and academic activities. He is principal investigator (PI) for a project funded by NUST. Recently, his biography has been published by South Asian Publication Who's Who in the World 2008 Edition and awarded with Star Laureate 2008 in recognition to his contributions to knowledge and research. Higher Education Commission of Pakistan has nominated him as their official PhD supervisor in 2010.

Currently, he is teaching various academic courses at MCS and supervising PhD and MS/ BE students in their final projects/thesis in NUST. He has organized 2 National conferences (NSEC 2010 and NCIA 2013). Presently is busy in arranging 2nd National Conference on Software Engineering (NSEC 2014) which is scheduled on 11-12 Nov 2014 at MCS, NUST. He presented his research paper in International Conference on Software and Data Engineering held in Dubai from 29-31 Jan 2012. He is authorized consultant for Nexsource Pak (Pvt) Ltd to design and develop a national level project for telemedicine system. He has published more than 35 research papers in international journals and conferences uptill now.

Mutahira N. Tahir(FM'87)was born in Rawalpindi on May 21, 1987. She got her Bachelors' degree in Software Engineering from Fatima Jinnah Women University, Rawalpindi Pakistanin 2011. She is currently doing MS Software Engineering from Military College of Signals (NUST). The major research field is software engineering.

She is currently doing MS software engineering. She has two research publications to her credit: "Challenges in Requirements Engineering for Mobile Applications for Disabled –Autism," Journal of Industrial and Intelligent Information . "Usability Issues for Smartphone Users with Special Needs-Autism," International Conference on Open Source Systems and Technologies (ICOSST). Her research interests are: software requirement engineering, usability engineering, software quality engineering and artificial intelligence.

Ms. Tahir paper had been accepted in IEEE conference naming International Conference on Open Source Systems and Technologies (ICOSST) "Usability Issues for Smartphone Users with Special Needs-Autism,"