International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 6– No. 9, March 2014 – www.ijais.org

Spambot Detection: A Review of Techniques and Trends

I.A. Adegbola
Dept. of Computer Science Emmanuel Alayande College of Education Oyo.

R.G. Jimoh
Dept of Computer Science
University of Ilorin

ABSTRACT
Spambot is a new way of creating and spreading spam using a robot in web 2.0 environment. Application such as blogs, face book, twitter and various form of social networking provides an enabling environment for spammers to deploy an intelligent program capable of imitating human behaviour to spread unsolicited message like spyware or malware and even content that can be use to perpetrate unwholesome act . This paper seems to harvest all past and current technique used in identification and detection of this type of spam and examine the trend in this type of spamming activities to suggest a research area for the researchers into spam management and detection.

General Terms
Techniques Review

Keywords
Antispam, Spambot, Detection, Behaviour, web 2.0 browser, Trend

1. INTRODUCTION
Spambot is a new way of creating and spreading spam using a robot in web 2.0 environment. Application such as blogs, face book, twitter and various form of social networking provides an enabling environment for this type of spam. A **spambot** is an automated computer program designed to mimic human behaviour in the sending and spreading of spam. Spambots usually create fraud accounts that can be use to send spam. This has been made possible with the advent of **web 2.0** a dynamic websites as opposed to static site. A Web 2.0 site permit users interaction inform of discussion and collaboration. They often share details and files with each other as can be seen in a social network sites like Face book Twitter, Application service provider. A Static site only permits passive content review. [19] This kind of spam that takes place on web 2.0 is generally referred to as spam 2.0. i.e a robot sending and spreading an unsolicited message in a dynamic sites [20,21]. Generically, this type of spam is detected by implementing the CAPTCHA test i.e *Completely Automated Public Turing test to tell Computers and Human Apart* (CAPTCHA). This is in form of question or test to differentiate web robots from human being [22]. However, from security point of view machine learning can bypass CAPTCHA and from usability point of view it disturb and inconvenient legitimate user. [1-3] So therefore it is not the best solution to blocking web robot. Spammers are using this weakness in CAPTCHA to deploy spam to a specific client with a decipher code to bypass CAPTCHA and Spambot attack may reach many unintended target in this era of web 2.0. Spambot may hide in a legitimate site misleading visitor to a malware site. This not only drive away visitor to this site but can as well make the site to be blacklisted.

2. PROBLEM STATEMENT
Web spamming in web 2.0 generally called spam 2.0 is gaining ground and the challenge response technique like CAPCHA use to detect this type of spam is more of a passive approach as spammer can bypass it. [1-3]. A proactive approach is required to combat this type of spam. This paper is setting the scene for the researcher to know where to direct their focus. This paper begins by looking at the various techniques ever used in classification and detection of Spambot in web 2.0. Activities and behaviour of Spambot in web 2.0 environment were examined and based on this review research area or the trend of spamming could be discovered.

3. Review of Techniques

3.1 Introduction
Currently, it is relatively easy to manage and filter ordinary e-mail spam content in a static site. This task is simply email content classification. However researchers are yet to properly investigate the detection and management of spam in web 2.0 generally refer to as spam 2.0. This review aim at given it the comprehensive attention it deserved by looking at the techniques ever used by researchers. Researcher believed that the topic of spam 2.0 has been investigated by few researchers and the field is still open for contribution. The table below listed relevant papers and technique applied in them on Spambot detection and management and weakness there in. This review is based on publications seen.

3.2 Table1: Spambot Detection Techniques

S/N	Spambot Detection Techniques	References
1	Completely Automated Public Turing test to tell Computers and Human Apart (CAPTCHA)	[1-3]
2	Detection of unseen and camouflaged web robots	[4]
3	Malicious web robot detection method based on HTTP headers and mouse movement	[5]
4	User web access logs techniques	[6], [7]
5	Web tracking system to track Spambot data HoneySpam2.0	[8]
6	Interaction with spam botnet controllers	[9]
7	Study of opinion spam in review-gathering websites	[10]
8	Identification of video spammers in online social	[11]

	network by means of a Support Vector Machine classifier	
9	Survey spam filtering techniques	[12]
10	Web Spam Detection by Learning from Small Labeled Samples	[13]
11	A Survey on Link Based Algorithm for Web Spam Detection	[14]
12	Web Spam Detection Using Link-Based Ant Colony Optimization	[15]
13	Effectively Detecting Content Spam on the Web Using Topical Diversity Measures	[16]
14	Multi-View Learning for Web Spam Detection	[17]

3.3 Analysis of the Table1

Generically most websites adopt (CAPTCHA) Completely Automated Public Turing test to tell Computers and Human Apart. A challenge-response approach to separate web robots from humans [8]. However, CAPTCHA inconveniences user and research shows that it can be bypass by machine learning algorithm. Therefore it is not a usable and secure solution for stopping Spambot. [1-3].

In an attempt to detect hidden and camouflaged web robots, Tan et al. [4] propose a framework that uses navigation pattern, session of action to detect web robots. Unfortunately this is a study of static websites as oppose to dynamic sites web 2.0 where a spam can mimic human user.

Another similar effort was that of Park et al. [5]. They use HTTP headers and mouse movement to detect a malicious web robot based on the type of request of web services However it was not tackling spam 2.0.

User Web Access logs was also propose by Yiquen et al.[6] and Yu et al. [7] as a trusted source to classify web spam from legitimate pages. This is a web spam classification as oppose to spambot detection.

HoneySpam 2.0 [8] is another work for tracking web spam data. The idea proposes was more of web usage data gathering and is similar to Gobel et al. It can only be able to get latest spam as oppose to spambot detection.

Gobel et al [9] proposes a template to improve spam filtering technique. He uses interaction with spam botnet controller as a source to get latest spam message.

Jindal and Liu [10] proposes a machine learning approach to differentiating opinion spam from legitimate spam in a review gathering websites.

Zinman and Donath [18] attempted to create a model to distinguish spam profiles from legitimate ones in Social Networking Services. Their machine learning based method uses content-based features to do the classification. This may not be able to detect and block unwanted comment in blog and unpermitted thread in an online discussion board.

Benevenuto et al. [11] provide a mechanism to identify video spammers in online social network by means of a Support Vector Machine classifier against content-based features

Heymann et al. [12] survey spam filtering techniques on the social web and evaluate a spam filtering technique on a social tagging system.

Jaber et al.[13] Proposes an automatic ways of generating web pages data as train data set for web spam classification using semi-supervised learning algorithm. This is a manual way of web page labelling which is time consuming and labour intensive but yet it is just an approach to classify web spam rather than Spambot detection which is the source of Web spam data.

Sree Vani et al. [14] Evaluate the strength of Linked based Technique in classifying web spam to reduce undeserved ranking in search engine result. Experimental results show that some of these techniques are working well and can find spam pages more accurate than the others. However this is just an evaluation of technique used in a particular type of web spam rather than detection of the spambot.

Apichat et al. [15] present a novel link-based ant colony optimization learning algorithm for spam host detection. The host graph is first constructed by aggregating pages' hyperlink structure. The proposed learning model provides much accuracy in classifying both normal and spam hosts.

Cailing Dong and Bin Zhou, [16] Studies various content-based and link-based features spam classification model. They conducted a thorough analysis of content spam on the web using topic models and propose several novel topical diversity measures for content spam detection. This is still an improvement on content detection as opposed to host detection which is the spambot.

Ali Hadian and Behrouz Minaei-Bidgoli [19] proposes a page-level classification approach to build fast and scalable spam filters. They show that each web page can be classified with satisfiable accuracy using only its own HTML content.

Mohammed et al. [17] investigated four different classification algorithms (naïve Bayes, decision tree, SVM and K-NN) to detect Arabic web spam pages in search engine, based on content and they find out that decision tree was the best. This is a good work at removing the biasness in search result as a result of web spam intrusion.

3.4 Deductive Activities of Spambot from the review

Given the dynamism of Web 2.0 environment where user can send and receive information and engage in so many business activities in real time, spammers are now using this opportunity to deploy spam that can imitate human user and participate in an online discussion, file sharing and other dynamic events that happen in web 2.0. environment. Pedram et al [23]. So therefore it is easy for spammers to deploy automated program using web 2.0 applications like social networking sites to navigate and spread spam message. This is the use of web robot called Spambot. They are built in such a way that they can infiltrate any sites and so many legitimate sites are at the cross road of loosing user or visitors since their integrity is called for a concern. This not only waste system resources but has a negative impact on a legitimate site. The evil intention of spammers and the problem cause by this type of spam calls for attention. If this is possible for spammers then it is imperative for researchers to design a detection system to distinguish the behaviour of human and spambot on the internet.

3.5 Trends of Spambot in Web 2.0 Environments

Generally most of the researchers are concentrating effort on a particular type of spam as showed in the review above e.g search engine document ranking, social network profile and so on and they are limited to web spam within that domain and so they have little perception of what a spambot in web 2.0 is. Some are busy with classification of spam content within the domain and that is why different techniques are emerging and will continue to emerge on content classification because spammers are wise and will continue to harness every possible way to spread the spam.

The trend of spamming now is using an automated computer program (web robot) to spread spam content. Therefore it is important for the researcher to concentrate effort on the source of the web spam .i.e the spambot or web robot as oppose to web spam content classification. This will enable researcher to propose a detection mechanism to detect and stop spam in web 2.0. The only proactive measure dealing with the web robot is Completely Automated Public Turing test to tell Computers and Human Apart (CAPTCHA) and from the review research shows that it is not reliable, it inconvenient users and not secure since it can even be decipher by a machine learning algorithm as state above [3]. It is now imperative for researcher to come up with an approach that will be scalable and robust enough to detect all type of spambot in web 2.0 domain.

3.5 Suggestion for further research

This paper is investigating spambot techniques, strength and weakness in web 2.0 and looking at the trends of this new type of spamming activities. Researchers observed from the related literature that classification technique is not a viable solution to spam management in web 2.0. It is suggested that research should be directed to detection of the source of this type of spam which is Spambot as oppose to the classification of content. Also spam behaviour in web 2.0 needs to be examined thoroughly if and only if we want to develop a robust mechanism that will not inconvenient user and that will stop this type of spam. In future researcher intend to come up with a detection system based on the spam behavior.

4. ACKNOWLEDGMENTS

Our thanks to the researchers whose work were review in this paper.

5. REFERENCES

[1] A. Luis von, B. Manuel, and L. John, "Telling humans and computers apart automatically," *Commun. ACM*, vol. 47, pp. 56-60, 2004.

[2] K. Chellapilla and P. Simard, "Using Machine Learning to Break Visual Human Interaction Proofs (HIPs)," in *NIPS*, 2004.

[3] Y. Jeff and A. Ahmad Salah El, "Usability of CAPTCHAs or usability issues in CAPTCHA design," in *Proceedings of the 4th symposium on Usable privacy and security* Pittsburgh, Pennsylvania: ACM, 2008.

[4] P.-N. Tan and V. Kumar, "Discovery of Web Robot Sessions Based on their Navigational Patterns," *Data Mining and Knowledge Discovery*, vol. 6, pp. 9-35, 2002.

[5] K. Park, V. S. Pai, K.-W. Lee, and S. Calo, "Securing Web Service by Automatic Robot Detection," *USENIX 2006 Annual Technical Conference Refereed Paper*, 2006.

[6] L. Yiqun, C. Rongwei, Z. Min, M. Shaoping, and R. Liyun, "Identifying web spam with user behavior analysis," in *Proceedings of the 4th international workshop on Adversarial information retrieval on the web* Beijing, China: ACM, 2008.

[7] H. Yu, Y. Liu, M. Zhang, L. Ru, and S. Ma, "Web Spam Identification with User Browsing Graph," in *Information Retrieval Technology*, 2009, pp. 38-49.

[8] P. Hayati, K. Chai, V. Potdar, and A. Talevski, "HoneySpam 2.0: Profiling Web Spambot Behaviour," in *12th International Conference on Principles of Practise in Multi-Agent Systems*, Nagoya, Japan, 2009, pp. 335-344.

[9] G. Jan, bel, H. Thorsten, and T. Philipp, "Towards Proactive Spam Filtering (Extended Abstract)," in *Proceedings of the 6th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* Como, Italy: Springer- Verlag, 2009.

[10] J. Nitin and L. Bing, "Opinion spam and analysis," in *Proceedings of the international conference on Web search and web data mining* Palo Alto, California, USA: ACM, 2008.

[11] F. Benevenuto, T. Rodrigues, V. Almeida, J. Almeida, C. Zhang, and K. Ross, "Identifying Video Spammers in Online Social Networks," in *AIRWeb '08* Beijing, China, 2008.

[12] H. Paul, K. Georgia, and G.-M. Hector, "Fighting Spam on Social Web Sites: A Survey of Approaches and Future Challenges," *IEEE Internet Computing*, vol. 11, pp. 36-45, 2007.

[13] Jaber Karimpour, Ali A Noroozi and Somayeh Alizadeh. Article: Web Spam Detection by Learning from Small Labeled Samples. *International Journal of Computer Applications* 50(21):1-5, July 2012. Published by Foundation of Computer Science, New York, USA.

[14] M. Sree Vani , R.Bhramaramba , D.Vasumati and O. Yaswanth Babu. Article: A Survey on Link Based Algorithm for Web Spam Detection . *International Journal of Current Engineering and Technology, Vol.3,No.2 (June- 2013).* Published by Inpressco International Press Corporation

[15] Apichat Taweesiriwate, Bundit Manaskasemsak, Arnon Rungsawang, "Web Spam Detection Using Link-Based Ant Colony Optimization," aina, pp.868-873, 2012 IEEE 26th *International Conference on Advanced Information Networking and Applications, 2012.*

[16] Cailing Dong, Bin Zhou, "Effectively Detecting Content Spam on the Web Using Topical Diversity Measures," wi-iat, vol. 1, pp.266-273, 2012 IEEE/WIC/ACM *International Conferences on Web Intelligence and Intelligent Agent Technology, 2012*

[17] Mohammed Al-Kabi , Heider Wahsheh, Izzat Alsmadi , Emad Al-Shawakfa, Abdullah Wahbeh , Ahmed Al-Hmoud. "Content-based analysis to detect Arabic web spam"Article: Published online before print April 19, 2012, doi: 10.1177/0165551512439173 *Journal of Information Science June 2012 vol. 38 no. 3 284-296*

[18] A. Zinman and J. Donath, "Is Britney Spears spam," in *Fourth Conference on Email and Anti-Spam* Mountain View, California, 2007.

[19] 031072208 (2005-10-01)."Web 2.0: Compact Definition".Scholar.googleusercontent.com. Retrieved 2013-06-15.

[20] P. Hayati and V. Potdar, "Toward Spam 2.0: An Evaluation of Web 2.0 Anti-Spam Methods " in *7th IEEE International Conference on Industrial Informatics* Cardiff, Wales, 2009.

[21] R. Cooley, B. Mobasher, and J. Srivastava, "Web mining: information and pattern discovery on the World Wide Web," in *Tools with Artificial Intelligence, 1997. Proceedings.,*
Ninth IEEE International Conference on, 1997, pp. 558-567.