Current Trends in Detecting Internet Water Army on Social Media Platforms and its Challenges: A Survey

D. Hamithra Jothi
PG Scholar,
Computer Science and Engineering,
Government College of Technology,
Coimbatore, India.

Prof. T. Rajasenbagam M.E.
Assistant professor
Computer Science and Engineering,
Government College of Technology,
Coimbatore, India.

***Abstract* — The stable nature of the Internet is being disrupted by the Internet water armies over decades. The exact detection of such Internet water armies is highly needed. The Internet water armies had invaded all sorts of digital communication platforms. The behavior of Internet water armies to manipulate the information have adverse impacts on the content reliability on these platforms. Social imbalance could also be caused owing to the increasing threat of diverting the public to trust unauthenticated information. A wide range of research is being conducted to invade the Internet water army and their impacts on the common people. This paper attempts to provide a survey on the evolution and proceedings in the field of Internet water army detection and the underlying challenges ahead owing to the complexity of the content's nature, coupled with models of theoretical origin and the combining applications with comparison.**

Keywords- Internet water army, social media, social spam, machine learning classification.

I. INTRODUCTION

Social media is a mighty weapon in today's world due to the greater speed of propagation of information on such platforms. The increasing risk of internet contamination by group of internet polluters who are paid to post irrelevant and misleading comments creates unnecessary chaos and virtual disruption. Now-a-days, these paid posters are majorly prevalent in China encompassing students and youth who are unemployed. This had led to the inequity of the internet of China which is now facing the heat of opinion manipulation to a considerable extent. According to Chen et al [20], the Internet water army refers to a "specific group of users employed by interest organizations or individuals to post purposeful comments and articles on the Internet". Their distinct behavior is avoiding outer exposure and widening social influence. The hanging scenario of Internet due to these spammers is a menace of recent light. The "Troops, Trolls and Troublemakers: A Global Inventory of Organized Social media Manipulation [44]" by the University of Oxford Computing Program is a notable report that analyzed the network campaigning activities of twenty eight countries which provided a precise study of social media manipulation with consideration of various Internet water armies in platforms like Facebook and Twitter and contributed important evidences which exposed the stepping of Internet water armies globally.

The water armies wrap themselves as normal users and supply the internet with adverse information over a short span of time in order to meet the target. This makes them possess more complicated features. To be precise, they employ the rumors to manipulate the opinion of general audience to make their views stronger. The thrust for this work is the untouched areas which surrounded Internet water armies. The remaining part of the paper is organized as follows: Section II shows the works related to this paper. Section III details the collection of data. Section IV analyses the SWAD model. Section V depicts the accurate experimental results. Section VI gives an idea to overcome the Internet water army. Section VII discusses the analysis of various methods used. The conclusion and future works of this paper along with the references made is contained in Section VIII.

II. RELATED WORKS

Timely identification of these astroturfers existed as an interesting area of research for various scholars over decades. The detection based on content and features prevailed a difficult thing owing to the dissimilarities among ordinary and spam content. By using the generalization of stacks, a categorization model with classifiers on text was proposed by G. Sakkis et al.[2]. Classification of email by spam filters was proposed by M. R. Islam et al. [13]. The detailed reports on harmful effects of internet water armies over societal inequality are found in [10], [14], [21], [30]. As of Today, detection of Internet water armies is mainly done by machine learning algorithms that included extraction of features and selecting right classifiers. Back Propagation Neural Network - BPNN was utilized by C.H.Wu [12] to filter out these water armies. Particle Swarm Optimization (PSO) was employed by Y. Zhang et al. [31] and A. R. Behjat et al. [19] that became a valid testimony in the detection of Internet water armies.

C.Chen et al. [20] served as a part of those Internet water armies for acquiring the base data which spurred the further study to figure out the features including the rate of propagation, interval limit of posting, active time of users etc. There also prevails various drawbacks circulating them including but not limited to the negligence of psychological aspects namely classification of different psychologies and the transformation processes of Internet water armies. With the aid of the network theory, an Internet water army detection model was formed from theoretical aspects [53] that analyzed subnetworks and links among various nodes in same as well as different subnetworks.

S.no	Reference	Techniques used	Observations
1	C. Chen et al. [20]	Pretended as a part of Internet water armies	Obtained the first-hand data
2	C. H. Wu [12]	Back Propagation Neural Network	Showed better accuracy results
3	Y. Zhang et al. [31] A. R. Behjat et al.[19]	Particle Swarm Optimization (PSO)	Great testimony in detection of Internet water armies
4	G. Sakkis et al.[2]	Generalization of stacks	Improved the effectiveness of filtering approaches
5	K. Lee et al. [18]	Application of "honeypots"	Found the relationship between followers and following
6	T. S. Moh A. J. Murmann [16]	Feature-based matrix	Employment of network-level metrics was made
7	S. Jeong et al. [41]	Employment of Social Status (SS), Triad Significance Profile (TSP)	Proposal of an ensemble technique was done
8	F. Wu et al. [38]	Approach based upon graph – structure	Demonstrated the inner connection between the spam text and spammers on Social sites
9	H. Shen et al. [43]	Multi-View Learning for Social Spammer Detection (MVSD)	Combination of user and network information were taken together
10	Z. Miller et al. [32]	Application of nearly 107 data-driven indices	Decreased the global nature of the model

Table 1: Comparison chart of various related works of internet water army detection.

III. COLLECTION OF DATA:

Identification of water armies from a great pool of internet users with 100% accuracy is a task of great difficulty when the data is improper. However, if data is obtained from authenticated sources, the chances of detection would soar high. Achieving exact information is very important for training the classifiers to make them suitable for machine learning algorithms. The artificial judgement mechanism was employed in studies [21],[40] to combat this problem since it is difficult to communicate with reliable sources. This would also reduce the accuracy of the classification vector between the water armies and normal users. To deal with a more convincing dataset, the paper [53] purchased Internet water army data from water army promotion companies post wide range of research and complex negotiations and then gathered the information on comments of microblogs that were posted on the Weibo website by water armies. The dataset was then prepared from the software of web crawling called Octopus by segregating the comments posted by normal users. Then, in order to adopt the algorithms of machine learning, the dataset was divided into two main aspects namely: training set and test set. This paper discusses two cases by fixing the ratio between the two sets as 70/30 and 80/20.

IV. ANALYSIS OF SUPERNETWORK BASED WATER ARMY DETECTION (SWAD) MODEL

Majority of the traditional methods in the social network analysis focused only on "who is responsible" for the problem and did not focus over other parameters like time, place, event, and psychology. Also, connection between these parameters were not considered. Motivated by the supernetwork theory, few scholars applied it in social network field, mainly for the cases of Internet public opinion networks, in order to analyze the mechanisms of interaction and the influences between various elements [12] – [15]. The constructed public opinion supernetwork contained the following subnetworks namely environmental subnetwork, social subnetwork, psychological subnetwork, and viewpoint subnetwork [12]. In the paper [53], to apply supernetwork theory to the problem, reconstruction of the structure of the network was made to establish a supernetwork based water army detection (SWAD) model. This model could be used to provide a detailed description for certain public opinion cases by taking into account the social, information, psychological, and viewpoint aspects. Here, the social subnetwork was set as the main subnetwork, to which the other subnetworks gets connected. Social Subnetwork indicated the relationship of reply between the users who participated in specific public opinion cases where each user was considered as node and each edge was the reply relation between them. Information Subnetwork measured the summary of information posted in a particular Internet public opinion case, where individual information was taken as node and the connections between intervals were not considered. Psychological Subnetwork represented the types of psychology of various users who were included in public opinion event, where the individual type is considered as a node and the process of transformation between them was set as the edges in which each psychological type was identified on the basis of a psychological lexicon. Negative Keyword Subnetwork measured the negative keywords that were included in the posts, where each negative keyword was set as a node and two nodes that had an edge connecting them were consisted to be contained in a similar post.

V. EXPERIMENTAL RESULTS

		SWAD [53]	Tian et al.[25]	Zhang et al.[42]	Dai and Wang[49]	Zhang and Lu[51]
ACCURACY	NB	87.65%	85.36%	89.40%	86.25%	87.09%
	NN	87.99%	86.89%	87.56%	87.39%	87.23%
	SVM	87.25%	85.89%	85.49%	85.98%	86.32%
PRECISION	NB	72.65%	70.23%	74.56%	70.05%	73.56%
	NN	73.65%	70.23%	75.89%	70.15%	71.28%
	SVM	70.87%	68.24%	70.48%	70.08%	72.98%
RECALL	NB	74.89%	66.93%	72.58%	68.29%	67.45%
	NN	74.18%	71.33%	72.88%	74.69%	71.66%
	SVM	73.29%	68.20%	68.93%	68.26%	66.77%
F1-SCORE	NB	73.77%	68.56%	74.23%	68.98%	70.23%
	NN	73.48%	71.86%	72.48%	72.69%	71.25%
	SVM	72.05%	68.35%	69.83%	68.11%	69.58%

Table 2: Confusion matrix results of models under the ratio between training and test sets of 70/30.

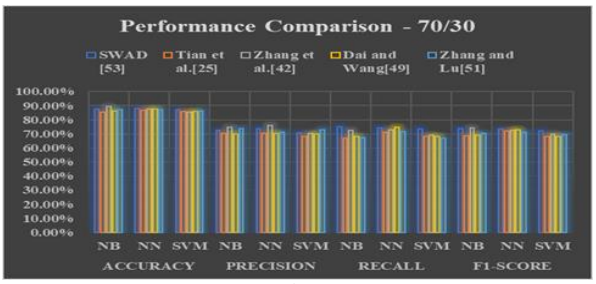

Figure 1: Bar graph showing results of selected Internet water army detection models under 70/30 ratio.

		SWAD [53]	Tian et al.[25]	Zhang et al.[42]	Dai and Wang[49]	Zhang and Lu[51]
ACCURACY	NB	88.25%	83.26%	88.26%	82.47%	88.49%
	NN	88.49%	84.65%	88.87%	81.09%	87.96%
	SVM	88.69%	83.29%	87.44%	81.48%	87.69%
PRECISION	NB	75.48%	66.59%	76.89%	60.25%	77.29%
	NN	76.41%	68.96%	74.89%	60.74%	74.55%
	SVM	74.93%	66.96%	72.88%	58.96%	74.75%
RECALL	NB	72.49%	50.02%	71.89%	60.08%	70.18%
	NN	74.25%	57.39%	71.93%	60.22%	71.63%
	SVM	73.28%	53.87%	75.64%	58.36%	67.19%
F1-SCORE	NB	73.87%	56.98%	73.58%	60.12%	73.47%
	NN	75.89%	62.42%	73.99%	60.89%	73.65%
	SVM	73.96%	60.08%	72.65%	58.97%	71.08%

Table 3: Confusion matrix results of models under the ratio between training and test sets of 80/20.

Figure 2: Bar graph showing results of selected Internet water army detection models under 80/20 ratio.

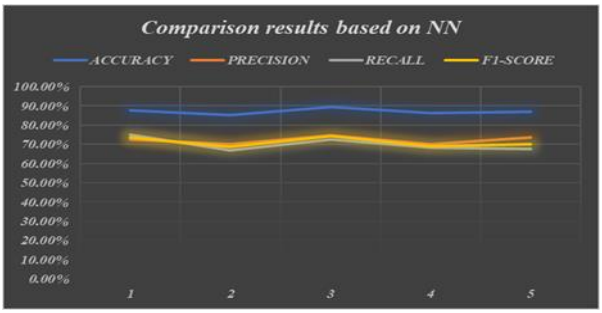

Figure 3: Comparison of results with NN

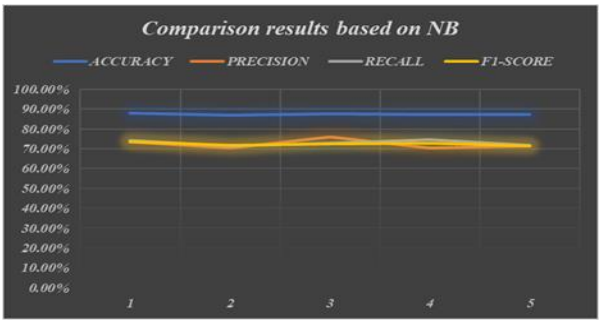

Figure 4: Comparison of results with NB

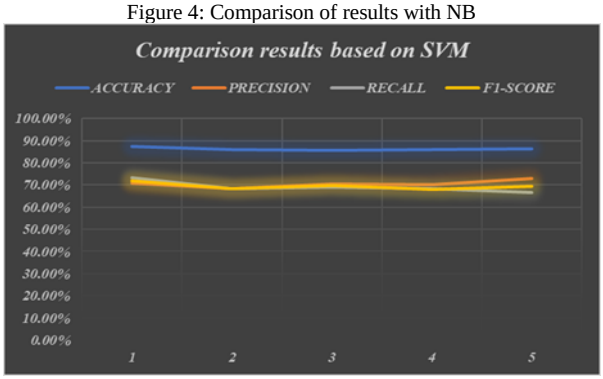

Figure 5: Comparison of results with SVM

VI. ANALYSIS OF METHODS USED:

In this paper, the commonly studied machine learning methods were utilized for training classifiers such as Neural network (NN), Naïve Bayes (NB) and the Support Vector Machine (SVM).

		SWAD [53]	Tian et al.[25]	Zhang et al.[42]	Dai and Wang[49]	Zhang and Lu[51]
NB	TP	955	823	916	872	830
	FN	300	402	320	385	385
	FP	320	348	215	326	298
	TN	4152	4026	4239	4158	4185
NN	TP	932	906	912	926	907
	FN	300	326	312	306	329
	FP	326	315	309	365	305
	TN	4178	4125	4198	4203	4136
SVM	TP	922	802	865	841	826
	FN	305	369	354	362	429
	FP	320	352	328	380	299
	TN	4122	4207	4169	4169	4220

Table 4: Confusion matrix values based on NN, NB, SVM.

These methods were used as they had shown a great performance in various papers focusing on detection of online water army detection [22], [36] recently. In Table 4, True Positive (TP) is the number of water armies that were rightly detected, the False Negative (FN) is the number of water armies that were wrongly detected, the False Positive (FP) is the number of non-water armies that were incorrectly detected, and True Negative(TN) is the number of non-water armies that were correctly detected.

VII. OVERCOMING INTERNET WATER ARMY

The Social Media Manipulation is a recurring problem whose heat is faced by users around the world. The methodologies to filter out the misleading information was recognized on various platforms with varying success degree. This paper had concentrated on the wide range of ways to detect and filter the Internet water army who engage in the social media manipulation. From various traditional approaches to current developments in this problem were identified and discussed. The existence of Internet water armies was found to be widespread in diverse media and applications like email, microblogs, social networking platforms etc. The posts were majorly accurate, sensitive, self-views which much belonged to different languages including typical vernacular and slang also embedded with sarcasm. They might even not be human understandable and are mainly machine comprehensive. This led to difficulty in the separation of features of social media content which was overcome in [53] which sorted them based on precise performance metrics.

VIII. CONCLUSION

The tug of war in between Internet water armies and researchers is a never-ending tale as they pose challenges to detect them by becoming smarter everyday. Hence, new theories are constantly blooming to reveal them thereby leading to regular surveillance through better scientific approaches. This survey attempted to stress the importance of various state-of-the-art techniques to identify the Internet polluters and provided a guideline on how to face the upcoming menace of Internet water armies by properly tuning the methods in order to get rid of the struggle.

REFERENCES

[1] G. Salton, A. Wong, and C. S. Yang, ‘‘A vector space model for automatic indexing,’’ Commun. ACM, vol. 18, no. 11, pp. 613–620, Nov. 1974.
[2] G. Sakkis, I. Androutsopoulos, G. Paliouras, V. Karkaletsis, C. D. Spyropoulos, and P. Stamatopoulos, ‘‘Stacking classifiers for anti-spam filtering of e-mail,’’ Int. J. Prod. Res., vol. 52, no. 19, pp. 5857–5879, 2001.

[3] A. Nagurney and J. Dong, Supernetworks: Decision-Making for the Information Age. Cheltenham, U.K.: Edward Elgar Publishers, 2002.
[4] H. P. Zhang, H. K. Yu, D. Y. Xiong, and Q. Liu, ''HHMM-based Chinese lexical analyzer ICTCLAS,'' in Proc. 2nd SIGHAN Workshop Chin. Lang. Process., Jul. 2003, pp. 758–759.
[5] T. Wakolbinger and A. Nagurney, ''Dynamic Supernetworks for the integration of social networks and supply chains with electronic commerce: Modeling and analysis of buyer—Seller relationships with computations,'' NETNOMICS, Econ. Res. Electron. Netw., vol. 6, no. 2, pp. 153–185, Aug. 2004.
[6] A. Nagurney, ''On the relationship between supply chain and transportation network equilibria: A Supernetwork equivalence with computations,'' Transp. Res. E, Logistics, Transp. Rev., vol. 42, no. 4, pp. 293–316, Jul. 2006.
[7] A.Nagurney, T.Wakolbinger, and L.Zhao,''The evolution and emergence of integrated social and financial networks with electronic transactions: A dynamic Supernetwork theory for the modeling, analysis, and computation of financial flows and relationship levels,'' Comput. Econ., vol. 27, nos. 2–3, pp. 353–393, 2006.
[8] Z. Yang, X. Nie, W. Xu, and J. Guo, ''An approach to spam detection by naïve bayes ensemble based on decision induction,'' in Proc.6th Int.Conf. Intell. Syst. Design Appl., Oct. 2006, pp. 861–866.
[9] A. Nagurney, Z. Liu, M. G. Cojocaru, and P. Daniele, ''Dynamic electric power supply chains and transportation networks: An evolutionary variational inequality formulation,'' Transp. Res. E, Logistics Transp. Rev., vol. 43, no. 5, pp. 624–646, Sep. 2007.
[10] P.Heymann, G.Koutrika, and H.Garcia-Molina,''Fighting spam on social Web sites: A survey of approaches and future challenges,'' IEEE Internet Comput., vol. 11, no. 6, pp. 36–45, Nov. 2007.
[11] X. I. Yun-Jiang and Y. Z. Dang, ''Method to analyze robustness of knowledge network based on weighted Supernetwork model and its application,'' Syst. Eng. Theory Pract., vol. 27, no. 4, pp. 134–140, Apr. 2007.
[12] C.H.Wu,''Behavior-based spam detection using a hybrid method of rule based techniques and neural networks,'' Expert Syst. Appl., vol. 36, no. 3, pp. 4321–4330, Apr. 2009.
[13] M. R. Islam, W. Zhou, M. Guo, and Y. Xiang, ''An innovative analyser for multi-classifier e-mail classification based on grey list analysis,'' J. Netw. Comput. Appl., vol. 32, no. 2, pp. 357–366, Mar. 2009.
[14] F.Liao, T.A.Arentze, and H.J.P.Timmermans, ''Supernetwork approach for multimodal and multiactivity travel planning,'' Transp. Res. Rec., vol. 2175, no. 1, pp. 38–46, 2010.
[15] G. Ruan and Y. Tan, ''A three-layer back-propagation neural network for spam detection using artificial immune concentration,'' Soft Comput., vol. 14, no. 2, pp. 139–150, Jan. 2010.
[16] T. S. Moh and A. J. Murmann, ''Can you judge a man by his friends? Enhancing spammer detection on the twitter micro blogging platform using friends and followers,'' in Proc. Int. Conf. Inf. Syst., Technol. Manage., Apr. 2010, pp. 210–220.
[17] X. Qin, N. X. Xia, and S. U. Yi-Dan, ''SVM-based social spam detection model,'' Appl. Res. Comput., vol. 10, pp. 765–767, Jan. 2010.
[18] K. Lee, B. D. Eoff, and J. Caverlee, ''Seven months with the devils: Along-term study of content polluters on Twitter,''in Proc.Int. AAAI Conf. Weblogs Soc. Media (ICWSM), Jul. 2011, pp. 185–192.
[19] A. R. Behjat, A. Mustapha, H. Nezamabadi-Pour, M. N. Sulaiman, and N. Mustapha, ''A PSO-based feature subset selection for application of spam/non-spam detection,'' in Proc. Int. Conf. Comput. Commun. Eng., Aug. 2012, pp. 675–679.
[20] C.Chen, K.Wu, V.Srinivasan, and X.Zhang,''Battling the Internet water army: Detection of hidden paid posters,'' in Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining, Aug. 2013, pp. 116–120.
[21] F.Ahmed and M.Abulaish,''A generic statistical approach for spam detection in online social networks,'' Comput. Commun., vol. 36, nos. 10–11, pp. 1120–1129, 2013.
[22] G. Stafford and L. L. Yu, ''An evaluation of the effect of spam on Twitter trending topics,'' in Proc. Int. Conf. Social Comput., Sep. 2013, pp. 373–378.
[23] P. H. B. Las-Casas, D. Guedes, J. M. Almeida, A. Ziviani, and H. T. Marques-Neto, ''SpaDeS: Detecting spammers at the source network,'' Comput. Netw., vol. 57, no. 2, pp. 526–539, Feb. 2013.
[24] Y. Ma, N. Yan, R. Yan, and Y. Xue, ''Detecting spam on Sina Weibo,'' in Proc. Int. Workshop Cloud Comput. Inf. Secur., Sep. 2013, pp. 404–407.
[25] X. Y. Tian, G. Yu, and P. Y. Li, ''Spammer detection on Sina micro-blog,'' in Proc. Int. Conf. Manage. Sci., Aug. 2014, pp. 82–87.
[26] I. Santos, I. Miñambres-Marcos, C. Laorden, P. Galán-García, A. Santamaría-Ibirik, and P. G. Bringas, ''Twitter content-based spam filtering,'' in Proc. Int. Joint Conf. SOCO'13-CISIS'13-ICEUTE'13, May 2014, pp. 449–458.
[27] K. Zeng, X. Wang, Q. Zhang, X. Zhang, and F. Y. Wang, ''Behavior modeling of Internet water army in online forums,'' IFAC Proc. Volumes, vol. 47, no. 3, pp. 9858–9863, Aug. 2014.
[28] N. Ma and Y. Liu, ''Superedge rank algorithm and its application in identifying opinion leader of online public opinion Supernetwork,'' Expert Syst. Appl., vol. 41, no. 4, pp. 1357–1368, Mar. 2014.
[29] R.-Y. Tian and Y.-J. Liu, ''Isolation, insertion, and reconstruction: Three strategies to intervene in rumor spread based on Supernetwork model,'' Decis. Support Syst., vol. 67, no. 2, pp. 121–130, Nov. 2014.
[30] Y. Liu, Q. Li, X. Tang, N. Ma, and R.Tian, ''Superedge prediction: What opinions will be mined based on an opinion Supernetwork model?'' ecis. Support Syst., vol. 64, no. 3, pp. 118–129, Aug. 2014.
[31] YZhang, S.Wang, P.Phillips, and G.Ji,''Binary PSO with mutation operator for feature selection using decision tree applied to spam detection,'' Knowl. Based Syst., vol. 64, pp. 22–31, Jul. 2014.
[32] Z. Miller, B. Dickinson, W. Deitrick, W. Hu, and A. H. Wang, ''Twitter spammer detection using data stream clustering,'' Inf. Sci., vol. 260, pp. 64–73, Mar. 2014.
[33] C.Fan, C.Liu, C.Zhang, and H.Wu,''Analysis of the time characteristics of network water army based on BBS information,'' in Proc. Int. Conf. Intell. Sci. Big Data Eng., Oct. 2015, pp. 20–28.
[34] G. Liang, W. He, C. Xu, L. Chen, and J. Zeng, ''Rumor identification in micro blogging systems based on users' behavior,'' IEEE Trans.Computat. Social Syst., vol. 2, no. 3, pp. 99–108, Sep. 2015.
[35] G. Wang, Y. Liu, J. Li, X. Tang, and H. Wang, ''Superedge coupling algorithm and its application in coupling mechanism analysis of online public opinion Supernetwork,'' Expert Syst. Appl., vol. 42, no. 5, pp. 2808–2823, Apr. 2015.
[36] A. Sharaff, N. K. Nagwani, and A. Dhadse, ''Comparative study of classification algorithms for spam email detection,''inefficient Identification of Users and User Sessions From Web Log Repository Using Dimensionality Reduction Techniques and Combined Methodologies. New Delhi, India: Springer, 2016, pp. 237–244.
[37] F. Gillani, E. Al-Shaer, and B. Assadhan, ''Economic metric to improve spamdetectors,''J. Netw. Comput. Appl.vol.65, pp.131–143, Apr.2016.
[38] F. Wu, J. Shu, Y. Huang, and Z. Yuan, ''Co-detecting social spammers and spam messages in microblogging via exploiting social contexts,'' Neurocomputing, vol. 201, pp. 51–65, Aug. 2016.
[39] M.Chakraborty, S.Pal, R.Pramanik,and C.R.Chowdary,''Recent developments in social spam detection and combating techniques: A survey,'' Inf. Process. Manage., vol. 52, no. 6, pp. 1053–1073, Nov. 2016.
[40] N.Wang, W.Xu, Z.Xu and W.Shao,''A survey on Supernetwork research: Theory and applications,'' in Proc. 35th Chin. Control Conf. (CCC), Jul. 2016, pp. 1202–1206.
[41] S.Jeong, G.Noh, H.Oh, and C.K.Kim,''Follow spam detection based on cascaded social information,'' Inf. Sci., vol. 369, pp. 481–499, Nov. 2016.
[42] X. Zheng, X. Zhang, Y. Yu, T. Kechadi, and C. Rong, ''ELM-based spammer detection in social networks,'' J. Supercomput., vol. 72, no. 8, pp. 2991–3005, 2016.
[43] H. Shen, F. Ma, X. Zhang, L. Zong, X. Liu, and W. Liang, ''Discovering social spammers from multiple views,'' Neurocomputing, vol. 225, pp. 49–57, Feb. 2017.
[44] M. Bradshaw and P. N. Howard, ''Troops, trolls and troublemakers: A global inventory of organized social media manipulation,''Univ.Oxford, New York, NY, USA, Tech Rep., 2017.
[45] N. Chavoshi, H. Hamooni, and A. Mueen, ''Temporal patterns in bot activities,''in Proc.26th Int.Conf. World Wide Web Companion, Apr.2017, pp. 1601–1606.
[46] S. Kwon, M. Cha, and K. Jung, ''Rumor detection over varying time windows,'' PLoS One, vol. 12, no. 1, 2017, Art. no. e0168344.
[47] Y. Lv, J. Liu, H. Chen, J. Mi, M. Liu, and Q. Zheng, ''Opinioned post detection in Sina Weibo,'' IEEE Access, vol. 5, pp. 7263–7271, 2017.
[48] I. Inuwa-Dutse, M. Liptrott, and I. Korkontzelos, ''Detection of spam posting accounts on Twitter,'' Neurocomputing, vol. 315, pp. 496–511, Nov. 2018.

[49] J.Daiand X.Wang,‘‘An identification model of water army based on data analysis,’’ J.Phys.,Conf.Ser.,vol.1069,no.1,Aug.2018,Art.no.012085.
[50] T. Wu, S. Wen, Y. Xiang, and W. Zhou, ‘‘Twitter spam detection: Survey of new approaches and comparative study,’’ Comput. Secur., vol. 76, pp. 265–284, Jul. 2018.
[51] W. Zhang and J. Lu, ‘‘An online water army detection method based on network hot events,’’ in Proc. 10th Int. Conf. Measuring Technol. Mechatron. Automat., Feb. 2018, pp. 191–193.
[52] X.Liu and C.Liu,‘‘Information diffusion and opinion leader mathematical modeling based on microblog,’’ IEEE Access, vol. 6, pp. 34736–34745, 2018.
[53] “An Internet Water Army Detection Supernetwork Model” Ying lian, Xuefan dong, Yuxue chi, Xianyi tang, and Yijun liu IEEE Access, May 6, 2019.