COOPERATIVE VECTOR BASED REACTIVE SYSTEM FOR PROTECTING EMAIL AGAINST SPAMMERS IN WIRELESS NETWORKS

P. MANO PAUL, R. RAVI
Research Scholar, Francis Xavier Engineering College, Anna University,
Vannarapettai, Tirunelveli, ph:9444412470, Email: manopaulp@yahoo.com, directorresearch@francisxavier.ac.in

Abstract: *Detection of spam emails is a key task since the internet community highly suffers from spam emails as nearly 90% of the incoming emails are spam. In this paper, a Cooperative Vector-based Reactive System (CVRS) has been proposed which filters spam emails in three steps, email classification, similarity detection and cooperative reaction. The CVRS system has been implemented at the receiver side with a group of reporters that evaluate the reactive feedback send by those reporters in a cooperative fashion. The CVRS model accurately filters spam emails without any delay. The CVRS system has been implemented using Map Reduce functionality and its performance has been evaluated using metrics such as false positive rate, false negative rate, detection accuracy and detection time. CVRS calculates feature probability on the clustered email, hence this creates only a short detection delay. Furthermore, CVRS system reduces the number of false positives and negatives by calculating similarity detection on the clustered email and thus achieves a high accuracy through validating the reporter's feedback result.*

Key words: *Similarity detection, vector, cluster, feature probability, spam email, reactive*.

I INTRODUCTION

Email is one of the most recognized forms of computer mediated communication [27] and they are commonly send in bulk with the intention of causing serious problems to the internet community. Studies show that more than 85% of the present email traffic is spam [5]. Emails are more vulnerable to malware attacks and they are generally sent in Multipurpose Internet Mail Extension (MIME) format through Simple Mail Transfer Protocol (SMTP) protocol. Spam emails devour the system's resources such as network bandwidth, storage space, traffic misuse, computational power, etc. Email service providers (Gmail, Hotmail, etc) are extremely affected and they are denied from servicing real users.

Spammers are eternally planning new ways to escape filters while anti-spam technologies [6] are available in many forms like, whitelist systems, disposable addresses, trusted-sender systems, blacklist systems, Reverse DNS systems, Reverse MX systems and lossless compression systems [28], [30] and these technologies cannot afford a complete solution. Several client-side email spam filtering tools are available currently and they became inaccurate today. Collaborative Spam filtering is used in Yahoo MailTM systems [14].

In this paper we present a Cooperative Vector-based Reactive System (CVRS) for Email Spam detection. This system performs email classification, similarity detection and cooperative reaction in a better way using Big Data analytic tools [8] to accurately filter out the spam emails. The email classification process uses Map Reduce tools [1] to extract the features and calculate the feature probability. The similarity detection process calculates the maximum feature similarity between two individual emails using Map Reduce tools. All incoming emails are defined in vector space so that detection is carried out in large space. The emails are clustered into five parts to reduce the detection time. The CVRS model performs similarity detection to reduce the number of false positives and false negatives and therefore achieves better detection accuracy.

Furthermore, the CVRS model performs reactive evaluation in collaborative manner to evaluate the reporter's trust level in validating an email. The CVRS model is dynamic and it uses Map Reduce tools using big data analytics which makes it to behave more effectively.

The rest of the paper has been organized as follows: Section 2 gives an overview of related works. Section 3 presents the proposed cooperative vector-based reactive system. Section 4 describes the experiments and performance results conducted and finally we conclude in section 5.

II RELATED WORK

The Autonomous decision making on Email Spam detection becomes less effective as decisions made by an individual or a single system cannot be trusted and needs to be validated. Existing researches proposed by [3], [4], [9], [24] focus on autonomous detection filters and they have proved their efficiency. A pipeline-based approach was proposed by [24] which uses a pipeline of filters such as DNS blacklist, SYN packet filter, network filter and content filters. Evolutionary multi-objective algorithms were presented by [9] to detect spam emails. A vector space model has been used by [10] for detecting spam emails. A GNUsmail framework was proposed by [3] for filtering spam

emails. A sender authentication network was developed by [4] for implementing the Sender Policy Framework (SPF) protocol for detecting spam emails. Word stemming approach [11] used hashing techniques for detecting spam emails. A feature set reduction approach was used by [7], [16] for detecting emails with malicious URLs.

Collaborative decision making offers best result on Email spam detection. Collaborative filtering of spam emails is a quite better and newer approach for email spam detection and it involves the cooperation of a group of agents about their decision in justifying an email as spam or non-spam. Vipul's razor, Distributed Checksum Clearinghouse (DCC), cloudmark, Spamnet, pizor [12] are most popular collaborative spam email filters. A number of researches on collaborative detection of email spam were carried out [12], [13], [14], [15] and they have proven their detection efficiency. The Particle Swarm Optimization (PSO) algorithm [17] generates random detectors in a Negative Selection Algorithm (NSA) in to improve the detection efficiency. In [12], a MIME fingerprint-based collaborative spam filter was proposed to detect spam emails. In [26], a hybrid model was proposed for detector generation that combines differential evolution (DE) and NSA algorithms for email spam detection. A signature was generated and distributed to related receivers of that email when a spam is detected [18]. A peer-to-peer-based reactive mechanism was proposed by [19] to detect spam emails in a collaborative fashion. A digest-based indexing scheme and a percolation search algorithm were proposed by [20]. Email fingerprints with multilayer decisions were proposed by [16] for email spam detection.

The existing approaches on email spam detection used different filters with different classifiers for classifying spam emails. These approaches have certain limitations which made them inaccurate and less efficient such as, increase in attack detection time, high false positive rate and false negative rate, decrease in detection accuracy. Most existing approaches were implemented at a single point which causes a burden on that point to handle huge tasks in less time. If the anti-spam filters were implemented in a collaborative fashion, it would provide better results. Therefore, we propose a novel Cooperative Vector-based Reactive System (CVRS) that initially performs email classification, followed by a similarity detection process and then finally performs a cooperative reactive process.

III. THE PROPOSED DEFENSE MODEL

The cooperative Vector-based Reactive System effectively and accurately classifies the spam and non-spam emails in three different steps: The Email Classification Process, The Similarity Detection Process and Cooperative Reactive Evaluation Process. The email classification process uses a vector space model [10] to represent the incoming email as vectors and extract the features [29] for feature classification. The similarity detection process measures the similarity of two emails using a soft cosine similarity measure [23]. The cooperative reactive evaluation process calculates a reactive function [13] for evaluating the accuracy of reactive result reported by different reporters. Figure 1 shows the architecture of CVRS model for email spam detection.

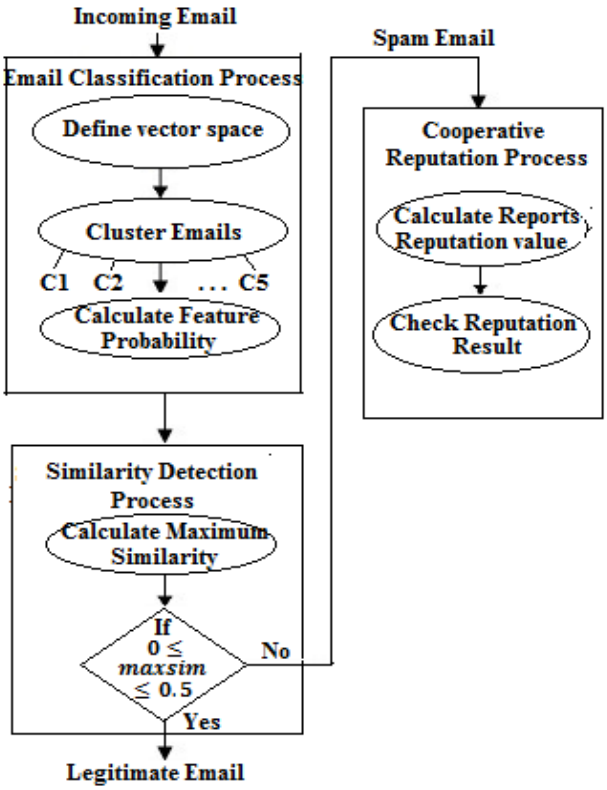

Fig. 1. The Architecture of CVRS System

3.1 The Vector Space Model

The incoming emails are represented as a 4-tuple $[E, C, (e, g), R]$. The tuple E represents a group of emails e, where $e: \{a_1, a_2, \ldots . a_n\}$ and each email consists of n number of a terms, tuple C represents a set of clusters of each email, $(C \in E)$, tuple (e, g) represents the similarity detection function that associates a spam email s, $(g \in M)$ that is previously categorized and an incoming email e, $(e \in E)$, tuple R is the reactive function that evaluates the reactive value of different reporters.

Every incoming email e_i is divided into k clusters and we represent $e_i = \{C_1, C_2, \ldots C_k\}$ as a set of clusters of e_i. Each email is represented as a feature vector, i.e., $\vec{e_i} = (w_{1ki}, w_{2ki}, \ldots w_{nki})$ where w_{jki} represents the feature weight assigned for feature a_j

in cluster C_k of email e_i. The feature weight is defined as, $w_{jki} = tf_{j,k,i} * idf_j$. Hence if j does not occur in cluster C_k of email e_i, then $w_{ikj} = 0$, otherwise $w_{ikj} > 0$ and the maximum normalization value is determined by w_{ikj}.

It is assumed that the features in the vector space are alphabetically ordered. The frequency of features in the entire email content is calculated in equation (1) as,

$$ff_{j,k,i} = \frac{a_{j,k,i}}{\sum_k a_{j,k,i}} * \frac{|E|}{|E: a_j \in C \in e|} \quad (1)$$

where $ff_{j,k,i}$ is the feature frequency, $a_{j,k,i}$ is the frequency of occurrence of feature a_j in cluster C_k of email e_i and $\sum_k a_{j,k,i}$ is the total number of features present in cluster C_k of email e_i, $|E|$ is the total number of incoming emails at the receiver and $|E: a_{j,k,i} \in C \in e|$ denotes the number of emails having the feature $a_{j,k,i}$.

3.2 Email Classification Process

During the email classification process, features are extracted from the incoming email as soon as they arrive and the stop-words [10], [21], [22] such as ('the', 'an', 'a', 'is') are removed so that the vector space model finds it easy for feature representation.

The stop words are removed from the dataset using an external stop-word list [10], [21], [22]. The features are then clustered into five different clusters, such as, email header, email body with plain text content, email body with html text content, attached files and embedded files.

Next, the feature probability FP(m) is calculated for each feature m in cluster k of email e_i and this is based on Information Gain (IG) and shown in equation (2). This helps to accurately classify the email feature as spam or non-spam. The use of clusters reduces the searching time and makes the feature probability calculation among clusters to function parallel. The feature probability is calculated as

$$FP(m) = \sum_{f_m \in k \in e_i} \sum_{C_i} P(f_m, C_i) * \frac{P(f_m, C_i)}{P(f_m) * P(C_i)} \quad (2)$$

where f_m is the mth feature value, C_i represents the class i to which the feature belongs, and $i = \{1,2\}$, $P(f_m)$ is the probability that the mth feature value is available in the training dataset, $P(C_i)$ is the probability that class C_i holds the training dataset and $P(f_m, C_i)$ is the probability that the mth feature value is in class C_i.

3.3 The Similarity Detection Process

During the similarity detection process, the maximum similarity of two emails, say, e_i and g_j is measured and detected. We obtain the maximum similarity of two emails (e_i, g_j) using soft cosine measure [23]. The soft cosine measure determines the similarity of feature pairs f_i and f_j in emails e_i and g_j. We define the soft cosine measure in equation (3) as,

$$sim(e_i, g_j) = \frac{\sum \sum_{i,j=1}^{N} g_{ij} e_{ij}}{\sqrt{\sum \sum_{i,j=1}^{N} g_{ij}^2} \sqrt{\sum \sum_{i,j=1}^{N} e_{ij}^2}} \quad (3)$$

where $e_{ij} = \sqrt{s_{ij}} \frac{e_i + e_j}{2}$ and $e_{ij} = \sqrt{s_{ij}} \frac{g_i + g_j}{2}$ and s_{ij} is the similarity of feature f_i and f_j. It is assumed that vectors e_i and g_j with n-dimensions are mapped to a new vector e_{ij} and g_{ij} with n^2 dimension. A threshold range between 0 and 0.5 is assigned as the maximum similarity threshold, and values beyond this range are definitely identified as spam emails.

The lowest threshold value is assigned as 0 and it is the highest possible value that creates no false negatives. The highest threshold value is assigned as 0.5 and it is the lowest possible value that creates no false positives. Therefore the similarity detection process is configured such that it reduces the number of both false positives and negatives.

3.4 The Cooperative Reactive Process

A Cooperative Reactive Process has been used as a final stage of evaluation of an email as spam or non-spam. During this process, the reporter's reactive result is determined for every incoming email. The cooperative reactive function evaluates the correctness of different reporters' trust in classifying an email and is defined in equation (4). This is done by calculating every reporter's trust on exploring an email based on its feature probability. When a spam email is detected, the reactive result is computed and distributed to appropriate receivers of that email. This can be defined as,

$$RR(i, m) = \sum_{U_R \in R(e_i)} \left(trust(U_R) * FP_i(m)\right) \quad (4)$$

where $RR(i, m)$ is the reactive result of feature m in email i, $trust(U_R)$ is the reactive value of reporter U_R and $FP_i(m)$ is the feature probability of feature m of email i. The reactive value of reporter U_R is shown in equation (5) and is defined as,

$$trust(U_R) = Rep(s, t-1) + \alpha(s, t) * F_{s,t}(e_i) \quad (5)$$

where $\mathrm{Rep}(s,t-1)$ is the reporter's reactive value that was calculated previously at time $t-1$, with the reporter's feedback signal, $\alpha(s,t)$ is the weighing factor of $\mathrm{Rep}(s,t-1)$ to balance the feedback result. The weighing factor $\alpha(s,t)$ in equation (6) is defined as,

$$\alpha(s,t) = \log\left(1 + \mathrm{count}(s) * \left|\sum_{i=1}^{s} f_{s,i}(e_j)\right|\right) \qquad (6)$$

where $\mathrm{count}(s)$ is the total number of feedback signals for email e_i if it is spam. $F_{s,t}(e_j)$ represents the reporter's feedback result for e_i. If $F_{s,t}(e_i) = 1$ then the feedback is accurate or else if $F_{s,t}(e_i) = -1$, then the feedback is inaccurate.

The Cooperative Reactive process increases the reporters trust on accurately confirming the reactive result in classifying an email as spam or non-spam. This process leads to better detection accuracy on detecting spam email.

IV PERFORMANCE RESULTS

The CVRS Model is implemented using Map Reduce functionality of Hadoop framework and the results were presented. The email classification process implements the map function using map class and the similarity detection function implements the reduce function using the reduce class. Here the accuracy, time and efficiency for the probable features of CVRS feature extraction has been verified by various metrics: False Positive Rate(FPR), Flase Negative Rate(FNR), Detection Accuracy and Detection Time. Moreover the CVRS model is compared with VSM [10] and PM [24] for effectiveness and we show that CVRS outperforms PM and VSM. We executed CVRS in Intel i3 processor at 2.5 GHz speed with a slot of 4GB RAM for its execution.

FPR [25] is defined as the number of benign emails that are wrongly classified as spam.

$$\mathrm{FPR} = \frac{\text{number of benign emails misclassified as spam}}{\text{total number of benign mails}} \qquad (7)$$

We show the number of false positives obtained for 10000, 20000, 30000, 40000 and 50000 incoming emails at different time intervals as shown in Table 1.

We found that the FPR value decreases with less number of received emails and it increases with more number of email received.

Table 1
Number of False Positives

Number of Emails	Number of False Positives		
	CVRS	VSM	PM
10000	1089	2124	2650
20000	2259	4671	6014
30000	3984	7774	9911
40000	5015	10184	13501
50000	6029	15560	18034

This is because with less number of emails the number of false positives decreases which leads to a decrease in FPR value and with more number of email received the number of false positives increases which leads to the increase in FPR value. The comparison of CVRS with VSM and PM is Shown in Figure 2.z

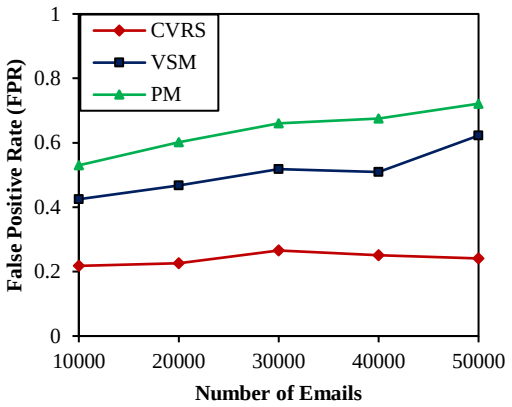

Fig. 2. Comparison of FPR

We observe that CVRS model generates a FPR of 0.14 and 0.3 whereas PM obtained a FPR of 0.45 and 0.65 and VSM obtained an FPR as 0.35 and 0.49 for 10000 and 50000 emails respectively. When compared with PM and VSM, the CVRS model outperforms the other two models. It is also observed that CVRS model generates less number of false positives and outperforms the existing methods. This is because of the n^2 dimensional mapping of vectors used in the similarity detection process that captures all the similarity between two emails. Moreover, the lowest threshold value used for similarity detection reduces the number of false positives. FNR [25] is defined as the number of spam emails that are wrongly classified as benign.

$$\mathrm{FNR} = \frac{\text{number of spam emails misclassified as benign}}{\text{total number of spam mails}} \qquad (8)$$

We show the number of false negatives obtained for 10000, 20000, 30000, 40000 and 50000 incoming emails at different time intervals in Table 2. We found that the FNR value decreases with less number of received emails and it increases with more number of email received. This is because with less number of emails the number of false positives decreases which leads to a decrease in FNR value and with more number of emails received the number of false positives increases which leads to the increase in FNR value. The comparison of CVRS with VSM and PM is Shown in Figure 3.

Table 2
Number of False Negatives

Number of Emails	Number of False Negatives		
	CVRS	VSM	PM
10000	274	327	456
20000	589	832	1317
30000	1124	1649	2469
40000	1883	3216	5371
50000	3017	5470	8642

We observe that CVRS model generates a FNR of 0.02 and 0.18 whereas PM obtained a FNR of 0.24 and 0.58 and VSM obtained an FNR as 0.16 and 0.4 for 10000 and 50000 emails respectively. When compared with PM and VSM, the CVRS model outperforms the other two models.

It is also observed that CVRS model generates less number of false positives and outperforms the existing methods. This is because of the n^2 dimensional mapping of vectors used in the similarity detection process that captures all the similarity between two emails. Moreover, the lowest threshold value used for similarity detection reduces the number of false negatives

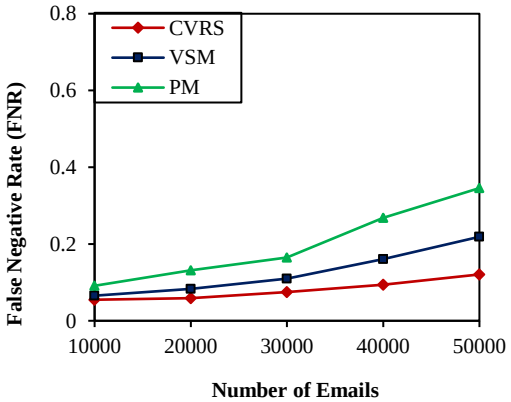

Fig. 3. Comparison of FNR

We define the detection time as the time taken to identify a spam email at the receiver in seconds. We show the detection time comparison of CVRS, VSM and PM in Figure 4 for 10000, 20000, 30000, 40000 and 50000 incoming emails.

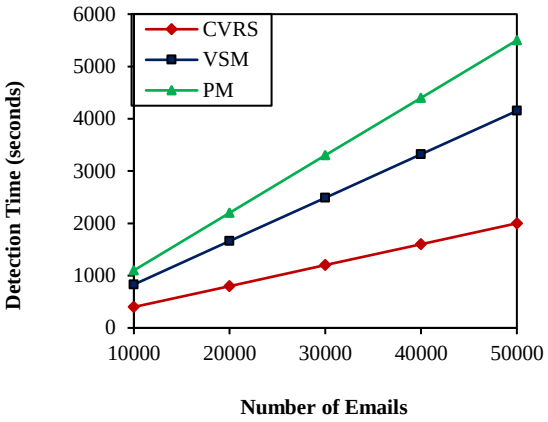

Fig. 4. Comparison of Detection Time

The detection time depends on the efficiency of the CVRS algorithm and the processor speed. The algorithm performs clustering of emails during the email classification process which speeds up the feature probability calculation and this causes a short delay in email spam detection.

It is observed that CVRS outperforms the other two methods by creating only a short detection delay. The results show that CVRS takes 0.04 seconds to detect a spam email, whereas VSM takes 0.83 seconds and PM takes 0.11 seconds. Thus CVRS achieves a short detection delay

The Detection Accuracy metric depends on FPR and FNR values. Obtaining maximum detection accuracy is the goal of CVRS insignificant false positives and false negatives. CVRS achieves better detection accuracy when the values of FPR and FNR are lower, and vice versa. We define the DA shown in equation (10) as,

$$DA = 1 - \left(\frac{FPR + FNR}{N}\right) \times 100 \qquad (9)$$

We compare DA of CVRS, VSM and PM for different number of incoming emails and the comparison is shown in Figure 5 .

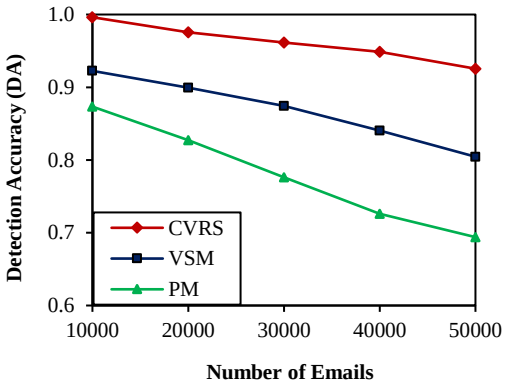

Fig. 5. Comparison of DA

We found that when the number of incoming

emails is less, the DA increases and it decreases with more number of incoming emails. This is because, DA depends on FPR and FNR values and hence with less number of incoming emails, the FPR and FNR values is less leading to an increase in DA and with more number of incoming emails, the FPR and FNR values increases leading to a decrease in DA. The results show that CVRS generates a DA of 0.96, whereas VSM generates a DA of 0.8 and PM generates a DA of 0.67 with 50000 emails respectively. CVRS achieves good DA and outperforms the other two existing methods. This is because of the threshold values in the range 0 to 0.5 which enables CVRS system to generate less number of false positives and false negatives with increase in DA.

V CONCLUSION

Thus a novel Cooperative Vector-based Reactive System (CVRS) has been proposed for filtering spam emails. The CVRS system is a cooperative technique engaged by a group of reporters in defending the spam emails. CVRS uses big data analytics and has been implemented using Map Reduce concept for defending spam emails. The performance of CVRS has been assessed using FPR, FNR, DA and detection time. It has been clearly shown that CVRS achieves good detection efficiency with less number of false positives and false negatives. Furthermore, CVRS achieves high detection accuracy with short detection delay.

Acknowledgement

We would like to thank the reviewers for their valuable comments.

References

1. M. AlMadahkah.: *Big Data In computer Cyber Security Systems*, In: International Journal of Computer Science and Network Security, vol. 16, No. 4, 2016, p. 56-65.
2. A. S. Aski., N. K. Sourati.: *Proposed efficient algorithm to filter spam using machine learning techniques*, In: Pacific Science Review A: Natural Science and Engineering, vol. 18(2), 2016, p. 145-149.
3. J. M. Carmona-Cejudo., M. Baena-Garcia., J. D. Campo-Avila., R. Morales-Bueno., A. Bifet.: *GNUsmail: Open Framework for On-line Email Classification*, In: ECAI 2010, 2010, p. 1141-1142.
4. G. Dalkilic., D. Sipahi.: *Spam Filtering with Sender Authentication Network*, In: Computer Communications, vol. 98, 2016, p. 72-79.
5. S. Nizamani., N. Memon., M. Glasdam., D. D. Nguyen.: *Detection of fraudulent emails by employing advanced feature abundance*, In: Egyptian Informatics Journal, vol. 15, 2014, p. 169–174.
6. S. L. Pfleeger., G. Bloom., *Canning Spam.: Proposed Solutions to Unwanted Email*, In: IEEE Security & Privacy, vol. 3 (2), 2005, p. 40-47.
7. Ranganayakulu., Chellappan.: *Detecting Malicious URLs in E-Mail-An Implementation*, In: AASRI Procedia, vol. 4, 2013, p. 125-131.
8. L. Varghese., M. H. Supriya.: *Spam: A Big Data Challenge*, In: International Journal of Advanced Research in Computer Science, Vol. 8 (1), 2017, p. 194-198.
9. Vitor Basto-Fernandes., Iryna Yevseyev., José R. Méndez., Jiaqi Zhao., Florentino Fdez-Riverola., Michael T.M. Emmerich.: *A spam filtering multi-objective optimization study covering parsimony maximization and three-way classification*, In: Applied Soft Computing, Vol. 48, 2016, p. 111- 123.
10. Carlos Laorden., Xabier Ugarte-Pedrero., Igor Santos., Borja Sanz., Javier Nieves., Pablo G. Bringas.: *Study on the effectiveness of anomaly detection for spam Filtering*, In: Information Sciences, Vol. 277, 2014, p. 421–444.
11. D. K. Renuka., T. Hamsapriya.: *Email classification for Spam Detection using Word Stemming*, In: International Journal of Computer Applications, Vol. 1, No. 5, 2010, p. 45-47.
12. Wenxuan Shi., Maoqiang Xie., Yalou Huang.: *Collaborative Spam Filtering Technique Based on MIME Fingerprints*, In: Proceedings of the 8th World Congress on Intelligent Control and Automation, Taipei, Taiwan, 2011.
13. Wenxuan Shi., Maoqiang Xie., Yalou Huang.: *Cooperative Anti-Spam System Based on Multilayer Agent*, In: Proceedings of the WWW 2011, Hyderabad, India, 2011, p. 415-419.
14. Joshua Attenberg., Kilian Weinberger., Anirban Dasgupta., Alex Smola., Martin Zinkevich.: *Collaborative Email Spam Filtering with the Hashing Trick*, In: proceedings of the Sixth Conference on Email and Anti-Spam CEAS, Mountain View, California, USA, 2009.
15. Sindhura Parvathaneni.: *Collaborative Spam Filtering*, In: International Journal of Engineering Research and Applications (IJERA), Vol. 1, No. 3, 2011, p.427-431.
16. Wenxuan Shi., Maoqiang Xie.: *A Reputation-based Collaborative Approach for Spam Filtering*, In: AASRI Procedia, Vol. 5, 2013, p. 220 – 227.
17. Idris., A. Selamat., N. T. Nguyen., S. Omatu., O. Krejcar., K. Kuca., M. Penhaker.: *A combined negative selection algorithm–particle swarm optimization for an email spam detection system*, In: Engineering Applications of Artificial Intelligence, Vol. 39, 2015, p. 33– 44.
18. Alan Gray., Mads Haahr.: *Personalised, Collaborative Spam Filtering*, In: Proceedings of the First Conference on Email and Anti-Spam (CEAS), Mountain View, CA, USA, 2004
19. Ernesto Damiani., Sabrina De Capitani di Vimercati., Stefano Paraboschi., Pierangela Samarati.: *P2P-Based Collaborative Spam Detection and Filtering*, In: Proceedings of the Fourth International Conference on Peer-to-Peer Computing, Zurich, Switzerland, 2004, p. 176 – 183.
20. Joseph S. Kong., Behnam A. Rezaei., Nima Sarshar., Vwani P. Roychowdhury., P. Oscar Boykin.: *Collaborative Spam Filtering Using E-Mail Networks*,

In: IEEE Computer Society, Vol. 39, No. 8, 2006, p. 67-73.
21. Gordon V. Cormack.: *Email Spam Filtering: A Systematic Review*, In: Foundations and Trends in Information Retrieval, Vol. 1, No. 4, 2006, p. 335–455.
22. Le Zhang., Jingbo Zhu., Tianshun Yao.: *An Evaluation of Statistical Spam Filtering Techniques*, In: ACM Transactions on Asian Language Information Processing, Vol. 3, No. 4, 2004, p. 243–269.
23. Grigori Sidorov., Alexander Gelbukh., Helena Gomez-Adorno., David Pinto., *Soft Similarity and Soft Cosine Measure: Similarity of Features in Vector Space Model*, In: Computacion y Sistemas, Vol. 18, No. 3, 2014, p. 491- 504.
24. T. Ouyang., S. Ray., M. Allman., M. Rabinovich.: *A large-scale empirical analysis of email spam detection through network characteristics in a stand-alone enterprise*, In: Elsevier Journal of Computer Networks, vol. 59, 2014, p. 101–121.
25. I Diana Jeba Jingle., Elijah Blessing Rajsingh.: *ColShield: an effective and collaborative protection shield for the detection and prevention of collaborative flooding of DDoS attacks in wireless mesh networks*, In: SpringerOpen Journal of Human-centric Computing and Information Sciences, Vol. 4, No. 8. 2014
26. Ismaila Idris., AliSelamat., SigeruOmatu.: *Hybrid email spam detection model with negative selection algorithm and differential evolution*, In: Engineering Applications of Artificial Intelligence, Vol. 28, 2014, p. 97–110.
27. J. M. Heisler., S. L. Crabill.: *Who are ''stinkybug'' and ''Packerfan4'' Email Pseudonyms and Participants' Perceptions of Demography, Productivity and Personality*, In: Journal of Computer-Mediated Communication, Vol. 12, 2006, p. 114-135.
28. Muthukumaran N., & Ravi R.: *The Performance Analysis of Fast Efficient Lossless Satellite Image Compression and Decompression for Wavelet Based Algorithm*, In: Wireless Personal Communications, vol. 81, no. 2, Print-ISSN: 0929-6212, SPRINGER, 2015, p. 839-859
29. Yesubai Rubavathi Charles., Ravi Ramraj.: *A novel local mesh color texture pattern for image retrieval system*, In: AEU—International Journal of Electronics and Communications. ISSN:1434-8411, 2016, p.225-233
30. Muthukumaran N., Ravi R.: *Hardware Implementation of Architecture Techniques for Fast Efficient loss less Image Compression System*, In: Wireless Personal Communications, Print-ISSN: 0929-6212, SPRINGER, 2015