Ying Tan

Anti-spam Techniques Based on Artificial Immune System

Contents

Preface

As the rapid developments of the Internet and mobile Internet, e-mails and instant messages have become most common and convenient media for our daily communications. However, spam, usually defined as unsolicited commercial or bulk e-mails, has been considered as an increasingly serious challenge to the infrastructure of the Internet, and severely intervened people's normal communications at work and life. According to the statistics from International Telecommunication Union (ITU), about 70% to 85% of the present emails in the Internet are spam. Numerous spam not only occupies valuable communications bandwidth and storage space, but also threatens the security of networking computer systems when it is used as a carrier of viruses and malicious codes. Meanwhile, spam wastes much users time to tackle with them, therefore decreases the productivity tremendously.

To fight against the spam, many solutions have been put forward to filtering spam off, which could be grouped as three categories: simple approaches, intelligent approaches and hybrid approaches. Simple approaches such as munging, listing, aliasing, and challenging, can be easily implemented while are also prone to be deceived by tricks of spammers. Intelligent approaches play an increasingly important role in anti-spam in recent years for their abilities of self-learning and good performance. However, a single anti-spam shield with one technique alone can be easily intruded in practice. Consequently, hybrid approaches by combining two or more techniques together are proposed in attempts to improve overall performance whilst overcoming the shortcomings of each single approach.

Among the varieties of anti-spam techniques, Artificial Immune System (AIS) inspired from Biological immune system (BIS), shows its excellence in performance and increasingly becomes one of most important methods to filter off spam.

The BIS is a dynamically adjusting system which is characterized by the abilities of learning, memory, recognition and cognition, such that it is good at recognizing and removing antigens effectively for the purpose of protection of the organism. Generally, the AIS is an adaptive systems inspired by theoretical immunology and observed immune functions, principles and models for problem solving, and is of a dynamic, adaptive, robust and distributed learning system. By mimicking BIS's mechanisms and functions, AIS is developed and now widely used in time-varying unknown environment for anomaly detection, fault detection, pattern recognition, optimization, learning, spam filtering, and so on.

The AIS features are just what an information security system such as spam filtering system needs, while the functions of BIS and information security system are very similar to some extent. Therefore, the biological immune principles provide effective solutions to computer security issues. The development of AIS-based information security systems, especially AIS-based anti-spam system, is increasingly receiving extensive attention. The application of immune principles and mechanisms can protect our computer and Internet network environment greatly.

Spam filtering is essentially a typical pattern recognition problem. To address the problem, many approaches have been proposed to filter spam from email traffics. In most cases, there are three main stages to achieve success, i.e. term selection, feature extraction, and classifier design. This book presents all of the three stages in detail. Specifically, as for term selection, this book presents a term space partition (TSP) approach, then a novel feature construction approach based on TSP, for a purpose of establishing a mechanism to make terms play more sufficient and rational roles in email categorization. As for feature construction, this book emphasizes on AIS-based feature construction methods which are the primary contents of this book and contain several feature construction approaches based on variety of immune concentrations. As for classifier design, this book shows that the mechanisms of danger theory are effective in combining classifiers. Finally, online implementation strategies of an immune based intelligent email server are developed under Linux operation system environment.

This book primarily consists of 13 chapters. The first two chapters briefly introduce anti-spam techniques and artificial immune system, respectively. From chapter 3 to chapter 9, immune inspired feature extraction methods from a variety of immune principles are elaborated, which include the feature extraction or construction approaches based on term space partition, global concentration, local concentration, multi-resolution concentration, adaptive concentration selection, variable length concentration, as well as parameter optimization of concentrations. The subsequent two chapters give two kinds of classifiers based on immune danger theory, i.e, immune danger theory based ensemble method and immune danger zone principle based dynamic learning method. The last two chapters describe immune based dynamic updating algorithm, AIS-based spam filtering system and its implementation.

All of the above contents came from our research work and the academic papers published by myself and my guided PhD and master students during the past decade. This book gives a panoramic image of spam filtering based on artificial immune system, which applied immune principles to feature attraction, classifier combination, and classifier updating, as well as online implementation for purpose of demonstrating the rationality of AIS methods for spam filtering.

In addition, the author presents those AIS-based anti-spam techniques in didactic approach with detailed materials and shows their excellent perfor-

mances by a number of experiments and comparisons with the state of the art anti-spam techniques.

Furthermore, a collection of references and resources is listed at webpages at http://www.cil.pku.edu.cn/resources/ and
http://www.cil.pku.edu.cn/publications/.

Nevertheless, there is still a long way to go for us to apply the immune based anti-spam techniques to the real-world mail filtering systems for a great advance.

The aim of this book is to provide a single collection of our proposed models and algorithms of anti-spam based on artificial immune systems during the past decade, which are scattered in a variety of academic journal papers and international conference papers, for academia, researchers and practitioners who are interested in the AIS-based solutions to spam filtering.

This book is intended to the audience who wishes to learn about the state of the art AIS-based anti-spam techniques. In order to understand the contents of this book comprehensively, the readers should have some fundamentals of computer architecture and software, computer security and spam filtering, artificial intelligence, computational intelligence, pattern recognition and machine learning.

Due to the limited specialty knowledge and capability of mine, a few of errors, typos and inadequacy must have in the book, some critical comments and valuable suggestions are warmly welcome. All comments and suggestions can send to ytan(AT)pku.edu.cn.

Finally, I, here, would like to deliver my heartfelt thanks to all who gave and will give a help in improving the quality of this book in advance.

Ying Tan
Beijing, China
April 15, 2015

About Author

Professor Ying TAN

Dr. Ying Tan is a full professor and PhD advisor at School of Electronics Engineering and Computer Science of Peking University, and director of Computational Intelligence Laboratory at Peking University (CIL@PKU: http://www.cil.pku.edu.cn). He received his BEng from Electronic Engineering Institute, MSc from Xidian University, and PhD from Southeast University, in 1985, 1988, and 1997, respectively.

His research interests include computational intelligence, swarm intelligence, data mining, machine learning, intelligent information processing for information security, fireworks algorithm, etc. He has published more than 280 papers, and authored/co-authored 6 books and 10+ chapters in book, and received 3 invention patents.

He serves as the Editor-in-Chief of International Journal of Computational Intelligence and Pattern Recognition (IJCIPR), an Associate Editor of IEEE Transactions on Cybernetics (Cyb), an Associate Editor of IEEE Transactions on Neural Networks and Learning Systems (TNNLS), etc. He also served as an Editor of Springer's Lecture Notes on Computer Science (LNCS) for 10+ volumes, and Guest Editors of several referred Journals, including Information Science, Softcomputing, Neurocomputing, IEEE/ACM Transactions on Computational Biology and Bioinformatics, Natural Computing, etc. He is the general chair of ICSI-CCI 2015 joint conference, and was the founding general chair of the series International Conference on Swarm Intelligence (ICSI 2010-2014), program committee co-chair of IEEE WCCI'2014, etc. He is a senior member of IEEE.

List of Figures

List of Tables

Symbols

Symbol Description

SC_i	presents the spam concentration of the ith local region	$tendency(t_i)$	presents the tendency of term t_i occurring in emails of a certain class
LC_i	presents the legitimate concentration of the ith local region	TR_s	presents the spam term ratio
DS_s	presents the spam detector set	TR_h	presents the ham term ratio
DS_l	presents the legitimate detector set	TD_s	presents the spam term density
		TD_h	presents the ham term density

1

Anti-spam Technologies

CONTENTS

Huge amount of spam not only wastes resources, but also brings severe threats to computer system security. To cope with these problems, researchers have conducted extensive researches on anti-spam technologies. This chapter presents the history, current situation and latest advances in researches on anti-spam technologies in detail. First, this chapter describes and discusses current anti-spam techniques, including legal means, email protocol methods, simple techniques and intelligent approaches. Then, intelligent anti-spam techniques, which are the most widely used and researched recently, are introduced and analyzed from two aspects, namely feature extraction approaches and classification methods. After that, performance evaluation methods and benchmark corpora for spam filtering are given. Finally, this chapter summarizes the current anti-spam techniques, and points out the directions of anti-spam researches in future.

1.1 Spam Problem

With the development of information technology and the popularity of the internet, email has been one of the most important communication tools. At the same time, the sending of numerous spam has made much trouble in e-mail communication, because these bulk emails not only waste communication bandwidth and storage, but also cost large resources of capital and time. Consequently, anti-spam is an urgent measure and becomes a hot research issue in the fields of computer and information security [200].

1.1.1 Definition of Spam

In 1978, email spam first appeared in Arpanet, bringing minor annoyance to the Arpanet users [32]. Nowadays email has gradually developed into a major means of peoples' communication, while the number of spam emails is increasingly expanded and the impact on people's daily life becomes more and more serious. Although the email has the diversity in form and content, but there is a clear distinction between the junk email and regular email. From email users' (recipients') point of view, the normal daily emails contain useful communication information, while meaningless information that users are not interested in constitutes junk emails. Different from the daily communication use of normal emails, the goals of sending large number of junk emails are usually business promotion, marketing, advertisement and others. In order to achieve real effectiveness of propaganda, the sending frequency of the same email is very high in huge scales.

Researchers usually define spam from the three general characteristics of above [175]. The classic definition of spam [47] is "unsolicited bulk email (UBE)", or "unsolicited commercial email (UCE)" by taking the business purpose of spam into account. Reference [67] defines spam as the emails whose users are not interested in, and spam can be regarded as the electronic version of traditional paper junk mail. Reference [7] gives the definition of spam from the perspectives of both sending behavior and content, and says spam are emails that are sent and spread in large amount but without permission of recipients. Reference [179] points out that spam has the following three aspects of characteristics: 1) The email is not associated with a specific user, and the user's identity has no relationship with the content of the email; 2) The recipient does not expressly consent to receive the email; 3) The content of the email does not make any sense for the recipient, and the recipient is also not interested in the email. Although there are some differences between these definitions, they all take users' experience into account during formulating features of spam. Spam is and will be only a burden to email users.

1.1.2 Scale and Influence of Spam

Compared with the traditional mail, email brings great convenience to our daily communication, for both reducing the communication cost and enhancing the communication efficiency. However, the features of low cost and fast speed of mail also make it convenient for spam senders to spread commercial advertising, bad information, and even computer viruses. Symantec report gives the statistics of the number and type of global spam email, and analyzes the current status of spam email [178]. Spam made up 67.7% of total emails in December, 2011; This ratio rose to 69% in January, 2012, for the spam senders' sending of large amount of commercials during the New Year period. As can be seen, the number of spam is very large, and spam has occupied most portion of the email traffic. The contents of spam are mainly related to pharmaceutical, watch, adult dating, weight loss, etc, where the number of spam that are related to pharmaceutical advertising is the most and makes up 38% of the overall spam. In addition to advertising, a small amount of spam involves malicious software, such as email virus and Trojans.

Commtouch Internet Threats Report [44] makes a statistical analysis of spam in the first quarter of 2012, pointing out that the number of spam has declined when compared to the same period of last year, but the average daily sending amount of spam is still up to 94 billion. Among all types of spam, the ratio of spam associated with pharmaceutical advertising has risen over that of the same period of last year, accounting for the overall proportion of 38.5%. The report also analyzes the domains of spam's header information, and concludes that the spam senders generally forge the header information of emails and the use of domain "gmail.com" gets the highest proportion when counterfeiting domain names.

Sophos Security Report [173] points out that spam senders often use viruses, worms, Trojan horses and other malicious programs to infect and damage others' computer systems and steal their user names and passwords, and even send spam by controlling those infected computers. Those infected computers essentially constitute a huge spam sending network, called as botnet by the researchers. This method is one of the primary means of sending spam emails, and botnets often contain a lot of junk emails. The botnet Rustock, which was closed in 2011, could send more that 30 billion spam in a day. When the botnet Rustock was closed, the global number of spam instantly noticeably declined. Sophos Security Report also analyzes the regional distribution of spam. According to the statistics in country, the US, India and Korea are the top three in sending number of spam. According to the statistics in continent, Asian has the largest sending number of spam, accounting for 45.04%.

With the growth of sending scale, the impact caused by spam has become more and more serious [175]. Ferris Research Group [154] points out, spam not only wastes network resources and affects network performance, what's more important, it also wastes a lot of users' valuable time to review and delete the spam, resulting in low productivity. They estimate that the waste

of resources caused by spam worldwide in a year is up to $ 130 billion. In addition, some spam comes with viruses, Trojans, worms and other malicious software, threatening the network security and user privacy. Symantec report [178] shows that there is one email containing the malicious software among every 295 spam and one phishing email among every 370 spam.

1.2 Prevalent Anti-spam Technologies

1.2.1 Legal Means

To deal with the massive losses resulted from spam, some countries have worked out corresponding acts to regulate the email sending field, attempting to narrow down the stream of spam. The US has, in 2003, formulated the Anti-spam Act — Controlling the Assault of Non-Solicited Pornography and Marketing Act, CAN-SPAM Act. Actions like forgery of mail header information, mail address fraudulence and mail address attacks are explicitly prohibited in this act. At the same time, business emails are required to be linked with the unsubscribe button or website. This rule in the act, however, as the document [74, 81] points out, has not the clear effect on the spam controlling, but has provided a way for the spam makers to conform the authentic or say effective mail addresses.

The 107th article of the Telecom Act of Australia has different requests for individuals and companies [74,143]. For individuals, only under the allowance of the recipient can spam producers send emails to them (including business emails, and emails to over 50 people). The requirements are relatively loose for companies and spam consisting of the unsubscribed links have their access to the business.

The European Assembly has passed, in June, 2002, the law and regulation on the privacy and electronic communication [25], which banned the sender to send spam without the permission of the recipient.

The formulation and implementation of these laws and articles have tackled some spam problems to some extent. These laws and regulations alone, however, can by no means completely eradicate the spam. Therefore, the combination of laws and regulations with other technical approaches are supposed to be the best way to better filter spam and guarantee the effectiveness of the email communications.

1.2.2 Email Protocol Methods

Email protocols control the delivery of email between the sender and recipient, including SMTP protocol (Simple Mail Transfer Protocol), POP protocol (Post Office Protocol) and IMAP protocol (Internet Message Access Proto-

col). SMTP protocol is used to control the delivery of email between MUA (Mail User Agent) and MTA (Mail Transfer Agent), and the delivery between two MTAs [111, 146]. POP protocol controls how to receive emails from MTA and put them into the local MUA [137]. According to the IMAP protocol, users can directly access remote MTA and read emails on the email server, instead of downloading emails to a local MUA [48].

Among these protocols, SMTP protocol is mainly used to control the sending and delivery of emails. Under this protocol, users can easily and conveniently interact with others by email communication. However, since the control strategy of this protocol is very simple, it brings an opportunity for spam senders. To effectively control sending of spam, there are two aspects of the SMTP protocol need to be improved [127]: On the one hand, during the delivery of emails, the unread emails are stored on the recipients' MTA, resulting in that the recipients would pay the price of the storage. Due to this strategy, the cost of sending spam is very low, which is one of the main reason of the massive flooding of junk emails. On the other hand, the SMTP protocol does not provide a valid sender authentication mechanism. According to the SMTP protocol, the email header information is basic text information and can be filled in by email senders at will, while the protocol does not provide verification mechanism. This makes it possible for spam senders to easily forge the email header information and successfully evade the filtering of those techniques based on header information.

To transfer the cost of sending spam to the email senders, reference [20] proposes a method to improve the way of email delivery: during the delivery process, emails are always stored on the senders' MTA until the recipients successfully finish receiving the emails. Reference [68] proposes a protocol in which the recipients could control the sending process of emails. When sent from strangers, the emails are first stored on the senders' MTA and the email summaries (or envelopes) are delivered to the recipients, and only when the recipients are interested in the emails, the emails are sent successfully. Reference [102] proposes a protocol where the email addresses are encapsulated. Under this protocol, when users publish their email addresses on the internet, information for restricting the use of the email addresses are encapsulated into the email addresses at the same time. When sent to these addresses, emails are verified according to the limit information encapsulated in the email addresses, and sent successfully only if they meet the limitation. This strategy could avoid the malicious use of email addresses. These methods for protocol improvement could theoretically achieve good effect as they control the mails from the source. However, it is too complicated to implement the improved protocols since it needs to upgrade the existing mail delivery facilities completely.

1.2.3 Simple Techniques

In the early days of the process of anti-spam studies, people have made out some simple countermeasures through observation of the basic features of spam and the cardinal methods of sending them. These simple ways in handling the spam have taken great effect.

1) Address Protection

Reference [94] mentioned a comparatively easier way in dealing with spam, which is to keep away the spam by changing the open email addresses. For example, converting the email address "usernamedomain.com" into "username#domain.com" or "username AT domain.com". And sometimes changing the "." into "DOT" can also work. By doing so, we can prevent the spam senders from getting the email addresses on websites through creeper skills. Nevertheless, the protective ability of this technology is too weak. The spam senders can still extract the real email addresses by simply adding some simple identification code when collecting email addresses. By now, through the dictionary attacks, the email address collection program can examine the ID number of the mail servers, as well as extract email addresses of the non-page documents (like DOCJPEGPDFXLSRTFPPT) on the internet.

2) Key-words Filtering

Key-words Filtering technology [45] is a way of judging the types of emails by testing whether or not there exists the words among the predefined ones, such as "invoice", "sales promotion", "Viagra", ect. At first, we use a complete match method. For example, "Viagra" can only match with "Viagra", and not applicable for "Viiaagra". But this method can be easily avoided for spam makers by making some small changes in the words. Later on, a so-called regular expression method is gradually accepted by many approaches. The particular mode of "V*i*a*g*r*a" can be matched with "V-i-agra", "Viiaagra" and "Viagra". This mode match method can effectively decrease the sphere of the key words and can be applied to the small changes of spam in some degree.

3) Black-list and White-list

Both of the two methods are based on the simple recognition the senders' identity. When information about identity is found to be forged, these two methods will lose their effect [160]. Black-list method is a way of filtering the spam by rejecting emails from specific IP addresses, TCP links, or domain names. But sometimes some information contained in the head of the email may be fabricated by the spam makers into other addresses. Thus the result is some innocent people's emails may be filtered altogether [93]. White-list method refers to a way of rejecting all the email resources, only allowing emails from the specific IP addresses, TCP links or Domain names. This is not a very convenient method to be used as it requires the two parties to send emails to each other for identity conformation.

4) Grey-list and Challenge-Response

Grey-list method will respond to those emails which are not within the

list of the server as the email is temporarily failing to be sent [225]. For those normal emails, the MTA will resend the email when it senses the response, that is, the server will resend it successfully on the reception of the email. But for spam, emails tend to be sent through open-relay, unable to be resent for wrongly responses, as a result of which the email cannot be reached by the recipients. The disadvantage of this method is that there will be some delay in sending normal emails.

Challenge-Response has added the challenge-response strategy on the basis of the white-list [209]. Likewise, this method has a white list. Email addresses from the white list will be successfully received. But when the addresses are the ones out of the list, the server will send to the sender a "Turing test". The email will arrive at the receiver on the condition that the sender has passed the test, and the corresponding sender's email address will be added to the original white list. Spam makers will usually adopt the forged senders' addresses to avoid the backwards traces, and are not expected to receive any returned tests.

On one hand, these two methods are responses made on the premise of the normal emails and spam, which takes advantage of the fact that spam cannot make response accordingly to judge the types of the emails. On the other hand, the process of making responses means to be delayed and occupy the bandwidth of the internet.

1.2.4 Intelligent Spam Detection Approaches

Intelligent spam detection approaches are the most effective and widely used technologies in the field. On one hand, intelligent detection approaches are highly automated and do not need much human intervention. But, on the other hand, intelligent detection approaches are characterized of high accuracy, robustness, strong noise tolerance and can adapt to the dynamic changes of the emails' content and users' interests.

In view of the intelligent approaches, spam detection is a typical classification problem, which could be solved by the supervised machine learning methods. Commonly, supervised machine learning methods extract discriminative information as features from the training sets and construct classifiers based on the features extracted according to the corresponding learning principles to classify newly coming email samples. Except for some human involvement during the process of training set generation, the learning and classification processes are completed automatically. Meanwhile, the learning model can adapt to the dynamic changes of emails' content and users' interests through adjusting the training sets and updating the classifiers [99,198]. A lot of classical machine learning methods have been successfully applied in spam detection [32, 45, 114], including Naive Bayes (NB) [40, 157, 169], Support Vector Machine (SVM) [22, 67, 109, 197], k-Nearest Neighbor (k-NN) [12, 83, 85, 158], Artificial Neural Network (ANN) [41, 199, 229] and Boosting [33, 91]. These methods have completed theoretical analysis and can achieve high perfor-

mance in spam detection, which endows them with good prospects of development. The following sections will concentrate on the intelligent spam detection approaches from two aspects, namely feature extraction and classification.

1.3 Email Feature Extraction Approaches

The feature extraction of an email is an essential part in a spam detection system. The accuracy, distinctiveness, robustness and adaptability of the feature extraction approach can affect the overall classification results and performance directly. According to the report by Chinese Internet Association in the fourth quarter of 2008 [174], the format of spam are mainly divided into three categories: text + image, text only and image only. This section reviews the classical feature extraction approaches based on text, image and behavior, respectively.

Before introducting the feature extraction approaches, let's talk about the term selection strategies (feature selection strategies) at first, which are indispensable and widely used in the process of feature extraction. Term selection strategies are used to evaluate the importance of a term or feature, or the quantity of information that a term or feature has, for the classification task to reduce the computational complexity and the possible effects from the noisy terms or features.

1.3.1 Term Selection Strategies

1) Information Gain (IG)

In information theory, the entropy is also known as Kullback-Leibler distance [232]. It can measure the distance of the sum of two probability distributions. In the studies on spam detection, it is used to measure the goodness of terms or features (discrimination). According to this strategy, when knowing whether a given term appears in an email, we can calculate the amount of information about the types of the receiving emails .

$$I(t_i) = \sum_{C \in \{c_s, c_l\}} \Big\{ \sum_{T \in \{t_i, \bar{t_i}\}} P(T, C) \log \frac{P(T, C)}{P(T)P(C)} \Big\} \tag{1.1}$$

where C represents the mail type, c_s and c_l indicate that the mail types of spam and legitimate email, respectively. t_i means the term appears in the email, while $\bar{t_i}$ shows the term t_i is not in the email.

According to this formula, the information entropy of each term will be calculated and the larger one will be selected to enter the next stage.

2) Term Frequency Variance (TFV)

Koprinska et al. [113] develops the term frequency variance (TFV) method

to select the terms with large term frequency variance. They think that terms with large term frequency variance contain more information. According to this strategy, these terms tending to appear in the same email type (spam or normal email) will be chosen while those with equivalent term frequency in the two types will be removed. In research of spam detection, term frequency variance is defined as follows.

$$T(t_i) = \sum_{C \in \{c_s, c_l\}} [T_f(t_i, C) - T_f^{\mu}(t_i)]^2 \tag{1.2}$$

where $T_f(t_i, C)$ is the occurrence frequency of term t_i, $T_f^{\mu}(t_i)$ is the average occurrence frequency of term t_i in both types of emails.

Reference [113] shows that the performance of TFV is better than IG in most cases. The top 100 terms of TFV and IG display that these terms have two characteristics: 1) frequently appearing in linguistics related emails; 2) appearing frequently in spam but rarely appearing in legitimate emails.

3) Document Frequency (DF)

Document Frequency is the total number of a specific term t_i over the whole training set [233]. According to this strategy, the term whose DF is larger than a threshold will be chosen. The definition of DF of term t_i is as fellows.

$$D(t_i) = |\{m_j | m_j \in M, and\ t_i \in m_j\}| \tag{1.3}$$

where M represents the whole training sets and m_j represents a single email in M.

DF indicates that the low-frequency terms have little information, so it will make no difference when these terms are removed. Ref [233] shows that when 90% of the low-frequency terms are removed, the performance of DF and IG is similar. The advantages of DF are its low computational complexity and linear proportional increase.

4) Other Term Selection Strategies

Term selection strategy plays an important role in the spam detection system [77,133,134]. In order to further understand term selection, three functions are listed below [25, 88, 233].

CHI: $\chi^2(t_i, c) = \frac{|M|(P(t_i,c)P(\bar{t}_i,\bar{c}) - P(\bar{t}_i,c)P(t_i,\bar{c}))^2}{P(t_i)P(\bar{t}_i)P(c)P(\bar{c})}$

Odds Ratio: $\tau(t_i, c) = \frac{P(t_i|c)}{1-P(t_i|c)} \frac{1-P(t_i|\bar{c})}{P(t_i|\bar{c})}$

Term Strength: $S(t_i) = P(t_i \in y | t_i \in x)$

In the above formulas, $C \in \{c_s, c_l\}$ are the types of emails and x and y represent two different kinds of emails in the training set, respectively.

1.3.2 Text Based Feature Extraction Approaches

The email feature extraction based on text usually contains two steps: 1) Term selection. According to the importance of terms, distinctive terms are chosen

to enter the next stage, as has been introduced above. 2) Feature extraction and display. The features of emails are extracted and displayed, which are expressed in a unified form.

1) Bag-of-Words (BoW)

This approach is also called vector space model, which is one of the most widely used feature extraction approaches in spam detection [9,10,82,88,103]. It converts each email into a n-dimension feature vector $< x_1, x_2, ..., x_n >$ through observing whether the term occurs in the email. In this approach, the value x_i of each X_i is the function of term t_i. And there are usually two types of representation for x_i: boolean type and frequency type [13]. In the boolean type, x_i is assigned as this mode: if t_i occurs in the email, then x_i is 1 and otherwise, x_i is 0. In the frequency type, x_i is the frequency of term t_i. In the experiments by Schneider, performance of the two representation types is similar [165].

2) Sparse Binary Polynomial Hashing (SBPH)

This method uses a sliding window to extract different features from emails [171, 235]. The N-term-length sliding window slides the email and each step it moves a term. In each sliding of the window, we extract 2N-1 features: the fresh terms into the window is reserved and other terms are reserved or deleted. And there are 2N-1 choices for the N-1 terms in the window, so we can obtain 2N-1 features. Then each feature is converted into a specific Hash value. After the extraction of features, the method will choose terms by the previous terms selection methods, which has a high precision but also a high computational complexity.

3) Orthogonal Sparse Bigrams (OSB)

In order to reduce the redundancy and complexity of SBPH, Siefkes [171] proposed orthogonal sparse bigrams (OSB) to extract a smaller feature set, which uses a N-term-length sliding window. What is different from SPBH is that only the common terms are extracted by OSB. For each window, the fresh term will be reserved for the common term and choose another N-1 terms to match it. As a result, each window can construct N-1 pairs of terms to reflect N-1 features. Compared with PSBH, it can reduce the number of features. Reference [171] shows that the performance of OSB is better than SBPH.

4) Artificial Immune System (AIS)

Oda et al. [140] designed an anti-spam immune system, which take advantage of regular expression to construct antibody (detector). The application of regular expression makes every antibody match massive antigen (spam), which can reduce the features effectively. Biological immune system (BIS) gives weights to each antibody. In the beginning of the algorithm, the entire antibody is initialized as default values. After a period of running, the weights of antibody matching more spam will increase and those matching legitimate emails will reduce. When the weights of antibody are less than the preset threshold, the antibody will be removed from the model.

More advances in research of AIS based spam filtering will be introduced in the next chapter.

1.3.3 Image Based Feature Extraction Approaches

Besides text content, emails sometimes contain image information. In normal emails, attached images are generally daily life photos about portraits, landscapes, architectures and others for daily communication in life and work; While in spam, images always contain advertising text information for the purpose of advertising and marketing [25, 75]. There are apparent differences between the spam images and normal images on the aspects of image attributes, colors, text, background, etc, and a number of image based feature extraction approaches have been proposed according to the significant differences between these two categories of images [16, 24].

1) Property Features of Image

Since spam is sent in huge quantities, spam senders usually control the size of the spam image by taking the network bandwidth and transmission efficiency into account. This makes the attributes of a spam image significantly different from that of a normal image. Reference [65] extracts the attribute information of images as feature vectors, including storage size, image length, image width, image compression formats and other information. Similar to the above work, Uemura et al. uses the image name, storage size as features and meanwhile adds the image compression rate information [208]. They point out that the spam image generally has a higher compression ratio than that of a normal image because the content of a spam image is relatively simple. Ref [115] employs similar attribute information as image features and analyzes the quantity of information that each attribute feature has by defining and calculating the noise ratio, which is associated with the email category information, of each attribute feature.

Reference [230] points out that the aspect ratio of a spam image is quite different from that of a normal image. There exist a large number of banner among the spam images and the difference between the length and width of a banner image is obvious. They take the number of banner images as a individual feature to construct the feature vector together with other features. He et al. compare images from the attributes like storage size, height, width, aspect ratio, etc, which are taken as preliminary features [92]. When it is difficult to determine the type of the email based on the above preliminary features, the color and histogram information are further extracted.

2) Color and Texture Features of Image

Byun et al. have noted that normal images have significantly different color features from spam images [31]. There are discriminations between the spam images and normal images in the aspects of color distribution, color intensity, etc, according to the histograms. The regional similarity of a spam image is high, while the spam images have color heterogeneity. The color saturation of spam images differs from that of the normal images [84]. This method divides the images into multiple categories by extracting these color features, where five types of spam images are included, like synthetic image, complex background image, etc, as well as three types of normal images, namely photograph,

map and comic. [131] pointed out that the smoothness of color distribution of spam images is not as good as normal images, because the spam images are generally synthetic and contain clear and sharp objects.

Wang et al.construct feature vectors by extracting the color histogram, direction histogram and coefficients of Haar wavelet transform and detect spam images with similarity comparison [223]. Since the number of spam emails sent is very large, spam images sent in the same batch generally have great similarities. In the training phase, similarity distances between the spam images and normal images are calculated and the minimum similarity distance is made threshold value. In the classification phase, similarities between the feature vectors of newly coming images and the vectors in the feature library are calculated, and categories of new images are achieved by weighted voting. Wu et al. [230] extract the vertical, horizontal and diagonal texture features of images by using wavelet transform. [76] points out that spam images mostly contain advertising information and are generally artificially generated, which result in that the spam images have different color and texture features from normal images. They extract features through global color histogram and gradient direction histogram, and classify the emails by using boosting methods.

Ref [215] incorporates the property information with color and texture information together to form the features of each image. The property information used in this method includes: image length and width, aspect ratio, image size, compression ratio and format information; the number of colors, primary colors, color saturation, etc, are used as color features; texture features are calculated by using the histogram method. Support vector machine (SVM) is utilized for classification after the feature extraction [195, 196]. Experimental results show that the hybrid types of features have better distinguishability than a single type of features. Huamin et al. [98] achieve higher accuracy by combining the text features, image property features and histogram features and integrating the multiple classifiers that are built. Li et al. [119] points out that global features and local features can reflect different sides of the image. They use the scale invariant feature extraction algorithm to extract the local features, then combine the local information with the global color and texture features and execute weighted classification according to the posterior probability.

3) Character Edge Features

On the basis of extracting edge of character vertically, Aradhye et al. [15] divide the image into text area and non-text area by calculating the similarity of character edge in each region and merging the similar regions. After the division, features of each image are constructed by calculating the size of text area in each image as well as the corresponding color saturation and color unevenness in text and non-text areas, respectively. Finally, the feature vector of an email is achieved by calculating the weighted sum of related features of all images included in the email according to the acreage of each image and support vector machine (SVM) [196] is employed for classification.

Wu et al. [230] give an effective method for detecting the text area. Firstly,

three feature pattern sets are established, namely local edge pattern, local edge concentration and global edge concentration. Boosting algorithm is used for generating detectors by training on the feature pattern sets to detect the text areas in images. Wan et al. [214] extract edge features by using color based edge detection method and corner information of character edge is also extracted in their work. Edges of characters and other objects are distinguished according to the corner information and width and height of the edges. Liu et al. [123] detect spam images through combing the text area features, which are edge information and corner information, and the color features.

4) OCR Based Features

Fumera et al. [72] extract the text information in images by using Optical Character Recognition (OCR) and the text information is further processed by adopting the text based approaches. Considering the high computational complexity of the OCR technology, they also point out this method should be combined with others and only applied to the emails that are hard to classify. However, they do not consider the influence of noise in spam images on the OCR technology as there hardly exists noise in spam images at that time. Biggio et al. [23] point out that the OCR based feature extraction appraoch could achieve good performance only when noise does not exist in the spam images.

To fight against the OCR-based detection method, spammers add noise information into the spam images, such as mixed fonts, background blur, text distortions and so on. However, these noise information has become the features distinguishing spam images from normal images. Biggio et al. [23] analyze the main principle of fuzzy techniques for spam images as well as the major impact of these techniques on fuzzy OCR process, and further extract the noise features by detecting abnormal in OCR processing steps. They propose a method to detect the noise in which the image is converted into a binary image and the vision complexity is calculated. Since the vision complexity of the normal image is located in a different range of values from that of the spam image with noise, we can extract noise features of character pieces and the background by utilizing this metric.

1.3.4 Behavior Based Feature Extraction Approaches

There are significant difference between spam and normal emails not only on the content, but also on the sending purpose, transmission method, interaction range, etc. In addition, spammers usually take certain measures to protect themselves to evade the spam filters. Thus, we can distinguish spam and normal emails by extracting different behavior features in the sending process of emails.

1) Behavior Features of Spammers

In the sending process, spammers forge the header information of emails to hide their identity. This makes the header information of spam has significant difference from that of normal emails, and the corresponding behavior

features of forgery could be extracted by analyzing the header information of emails [207, 234]. Yeh et al. [234] extract 17 behavior feature for spam detection by analyzing the abnormality of single entries and the effectiveness and consistency of cross entries, and obtain the 113-dimensional feature vector by sparse coding. Abnormality of single entry is discriminated by checking whether "From", "To", "Delivered-To", "Return-Path", "Date" and other information is abnormal, such as format correctness, whether it is empty, the time rationality and so on. Features of cross entries are obtained by checking the effectiveness and consistency of corresponding entries on type and format. Wu [229] adds the comparison of header information and system log on the basis of the above, and tells whether there is forgery by checking the consistency of the corresponding entry. Good performance is achieved by extracting the 26-dimensional behavior feature vectors and applying a hybrid model of rule processing and back-propagation neural network for classification, which further confirms the validity of such behavior features. In [6], information of the sending process is taken as behavior features, including the number of servers involved in mail delivery, mail transmission time, and sending the existence of domain names and others. Experiments show that adding these sending process information can effectively enhance the performance of the original behavior feature extraction methods.

Since the sending purposes of spam are similar and the sending behaviors have some similarities, some studies can filter spam by group from the perspective of similarity. Reference [118] studies the similarity of spam sending behaviors (eg, containing the same URL link), and filters spam by group according to the similarity. Through analyzing the characteristics of emails, it is found that there is a higher possibility for the spammers who appear in more than one group to send spam again. Ramachandran et al. [152] study the similarity of email sending mode. They define sending modes according to the sending frequency of an IP address to d different domains in the period t and adopt a clustering analysis on behaviors according to the sending modes. [8] analyzes the URL links in emails and clusters emails by tracking the located servers of the linked websites. They point out that one server usually provide service to numbers of linked websites of spam, allowing clustering emails according to the server information.

2) Network Behavior Features of Spam

Network features of spam and normal emails are quite different [153], and researches have extracted the related behavior features from the perspective of IP address, i.e., sending server, sending time, persistence and etc. [231] analyzes the login information of mailbox and changes in the login IP and concludes that most of the emails sent from dynamic IP addresses are spam, while nearly half of the Hotmail spam are sent from dynamic IP addresses, so it should be paid extensive attention to the dynamic characteristics when to extract the IP address related features. West et al. [227] find through analysis that there is a spatial similarity between spam addresses and they are always located in adjacent spaces though the spam sending addresses dynamically

changed. In addition, they found that the historical data in blacklist have a good reference value in the forecast. They propose a space-time evaluation method by combining spatial characteristics and historical data, whose error rate is half lower than that of traditional IP blacklist filtering .

Ramachandran and Feamster [151] study the characteristics of network behavior during the sending process of spam, and they specifically analyze the distribution of IP addresses that sending spam, situation of BGP (Border Gateway Protocol) routing hijack, persistency of spam sending hosts and characteristics of spam botnets. Through analysis, they obtain that the majority of spam comes from a small range of IP addresses (eg, 60. * - 70. *) and the spam sending process of botnet is not persistent. They point out that these network related features should be concerned about during spam filtering, and pay attention to identify botnets. [112] analyze the spam datasets from 2005 to 2009, and find that the distribution of IP addresses of botnets becomes more widespread in 2009 compared with that in 2006. This change will lead to a decline on the performance of IP address based filtering methods and makes it more difficult to control the botnets.

In [153], the network behavior features of spam are comprehensive analyzed, which includes the range of IP addresses, type of operating systems, geographical characteristics, sending modes, etc. Three unsupervised methods are utilized to analyze the association characteristics of the spam sending process. Duan et al. [69] systematically analyze the behavior characteristics of spammers from the perspective of the mail server and the network layer, such as the distribution of mail servers, the proportion of spam, the active time of spammers and so on. They point out that new methods on sender authentication mechanism and email sending control should be studied in order to effectively reduce spam.

3) Social Network Based Behavior Features

The sending and receiving networks of normal emails and spam are significantly different. Normal emails are generally used for interaction between friends, colleagues and relatives, forming normal social network features, while the spammer always needs to extract a large number of email addresses from web pages to send spam, forming abnormal interaction networks [27]. In [27], each email account is taken as a node and the edges between nodes are constructed in accordance with the sending and reception of emails. For the sending network of spam, the number of nodes in the network is large while the relation between adjacent nodes is relatively simple. The clustering coefficient calculation methods are given to distinguish normal email sending networks and spam sending networks according to interconnection of nodes and situation of shared nodes between adjacent nodes.

Based on [27], Lam et al. [116] construct social networks by extracting information from the interaction logs of emails determine whether an email address is used to send spam according to the characteristics of the social networks. This method extracts an 7-dimensional vector to express the social network characteristics of each email account, including the number of email

accounts that have sending-reception relations with this email account, the interaction frequency of this email account with others, etc. For a spammer account, the number of emails sent by this account will be very large while the number of emails received is very small, which makes it significantly different from the interaction process of normal emails. Debarr et al. [63] take the space distance into consideration when constructing the social network features, which is defined as the number of transit between two email accounts during the sending process of email.

Li et al. [121] consider not only the connection relationship between email accounts but also the metrics of intimacy of social relations and user interest in the process of constructing social networks. This algorithm requires user involvement and encourages users to provide their social information, such as hobbies, occupation, religion, family relationships and so on. Social relationship and closeness between email accounts are measured through these information. For email interactions between distant nodes, the algorithm performs more stringent checks. At the same time, this algorithm extracts user preference from user information and provides personalized spam filtering policies based on user preferences. In addition, the link weights between nodes are dynamically adjusted to avoid hijacking attacks of email accounts.

4) Immune Based Behavior Feature Extraction Approaches

Yue et al. [236] extract character information from IP addresses, SMTP marks, URL links and reply addresses, and computes the corresponding "spam score" of each part according to the character information and the designed feature calculation formula. These spam scores are combined to generate antibodies. On basis of this, the initial set of antibodies are adjusted by using the artificial immune network theory, and antibodies with high affinity are cloned and mutated by adopting the clonal selection algorithm, where the number of antibodies with low affinity are suppressed. Eventually, the antibodies of the immune network are clustered. The use of artificial immune network makes the behavior features with high affinity be preserved, while the behavior features with low affinity be filtered out.

1.4 Email Classification Techniques

1) Naive Bayes

Simple and effective, this method is the most common method due to its simplicity and effectiveness. Many studies have shown that this method is the most effective way of dealing with the spam, with relatively high precision rate and recall rate [11,157]. Some studies indicate that the application of the polynomial mode will acquire higher accuracy rate than that of the Bernoulli rate [165]. Variations have been derived from the traditional Naive Bayes. Raju Shrestha [170] has taken the advantage of the internal connection features of

the same key-words appearing in different places to calculate the co-weighting of the key-word and made great improvement in its property. Li [120] mentions the improved Naive Bayes more focused on the users' feedbacks which has acquired a comparatively low false positive and better performance.

2) k-Nearest Neighbors

Sakkis [158] has put into effect the k-Nearest Neighbors — kNN (a classical lazy learning method) in the scope of spam detection. They have studied the influence of domain (k), the characteristic dimension, and the practice set on the performance of the testing machine. The experiments has shown that the average performance and properties are better than Naive Bayes.

3) Boosting Trees

Schapire and Singer [163] are, for the first time, to apply this method in the area of text classification, which handles the problems of divisions of multi-class and multi-label through multi base hypotheses. Carreras and Marquez [33] have applied AdaBoost algorithm in email filtering. Based on two public data sets experiments (PU1 corpus and Ling-Spam corpus), they drew a conclusion that Boosting Trees method was better than Naive Bayes theorem, Decision Trees and kNN algorithms in performance. However, Nicholas [181] thought Boosting Trees and AdaBoost using decision stumps were worse than Naive Bayes in terms of accuracy and speed.

4) Support Vector Machine

Support Vector Machine (SVM) is deeply discussed in [66,210,211]. Drucker, et al. [67] have implemented a spam filter based on SVM. Their research shows that SVM filter and Boosting Trees can both meet the lowest error rates, while Boosting Trees spend more time in training process.

5) Ripper

Different from other classification methods, Ripper [43] concludes the rule of classification from training sample set without the help of feature vectors, which consists of the rules of if-then.

6) Rocchio

Classifier of this type [164, 180] uses the standardized TF-IDF as vectors of training samples. The advantage of the classifier lies in its fastness in training and testing, while the disadvantages can be seen from the following two aspects: extra training time is needed when searching for optimum threshold and β in training set, and also these parameters take on a weaker property of generalization.

7) Clustering

Minoru Sasaki et al. [162] present text clustering based on the feature space model, using spherical k-means to calculate different clusters and then tagging the extracted centroid vector according to its class by counting the distance between the vectors of the new emails and centroid vector. This method has shown a good detection performance on Ling-Spam corpus.

8) Meta-Heuristics

Chi-Yuan Yeh et al. [234], on account of the influence the variation of keywords has on the performance of the learning methods of key-words-based

robots, present the use of the behavior of spammers to classify emails. These behavioral characters are described through Meta-Heuristics. Under the given Meta-Heuristics, 113 new features have been extracted. The result shows that this method is superior to the filter type of key-words, and has also shortened the training time.

9) Artificial Neural Network

James Clark et al. [41], by using Artificial Neural Network (ANN), have made email classification automatic [155, 156, 186, 190, 193]. Linger, a system developed by them, has achieved a higher rate of accuracy, recall and precision. However, experiment on PU1 corpus has shown a performance reduction. Based on the descriptive properties of words and news, Iran Stuart et al. try to classify emails with the help of artificial neural network. The experimental results show that certain extension or modification of the feature set should be made for its improvement on performance.

10) Artificial Immune System

Andrew Secker [168] put forward the concept of AISEC (Artificial Immune System for Email Classification), aiming to distinguish emails the users are interested in and those they are not. Given that there is no repeating in training, this method can realize advanced email locator on ends, and track the change of the users' interests.

Terri Oda et al. [142] have applied this model in spam filtering, taking advantage of the detection principle of 'self/non-self' and the concept of detector. In the spam filtering system, a gene library is constructed from various sources, including the lexical vocabularies, words and expressions in the emails collected, contact information in spam, the header information of emails and so on. In the process of system initialization, antibody and its related lymphocyte are produced in a random way. In the process of construction, no similar antibodies are allowed to be produced repeatedly. Each lymphocyte, apart from its attribute of immunity, has another two attributes, namely, message-matched and spam-matched, signifying, respectively, the amount of emails matched to lymphocyte and that of spam. In the training process of lymphocyte, modifications on the property values of message-matched and spam-matched are made to the matched lymphocytes. In the process of system operation, the evaluation method of using the weighted average is adopted to sort emails. In this way, lymphocytes that have been matched for many times takes a larger proportion in the score.

More advances in research of AIS based spam filtering can be seen in the next chapter.

1.5 Performance Evaluation and Standard Corpora

1.5.1 Performance Measurements

Spam detection is still a hot topic in the information security, many novel anti-spam techniques are increasingly proposed and studied deeply. In order to make it easier to compare and choose a good way to filter spam, researchers gave a few measurements to make a comparison of the performance between different ways and systems for filtering spam. This section mainly introduces and analyzes some common ways to evaluate the performance of spam detection and give some public standard corpora.

1) Spam recall

Spam recall can figure out the rate of spam correctly spotted and categorized by the arithmetic model. The systematic model with high rate of spam recall can filter spam and reduce the bad influence made on people's life by them more effectively. The following formula is to calculate spam recall.

$$R_s = \frac{n_{s\to s}}{n_{s\to s} + n_{s\to l}} \tag{1.4}$$

where, $n_{s\to s}$ means the number of spam correctly spotted and categorized while $n_{s\to l}$ means the number of spam mistaken as normal mails.

2) Spam precision

Spam precision can figure out the precision of measuring spam. It can figure out the rate of spam correctly spotted and categorized. It can also reflect the rate of normal emails mistaken as spam. The higher the spam precision is, the less the number of normal emails mistaken as spam is. The following formula is for calculating the spam precision.

$$P_s = \frac{n_{s\to s}}{n_{s\to s} + n_{l\to s}} \tag{1.5}$$

where, $n_{l\to s}$ means the number of normal emails that are mistaken as spam.

3) Legitimate recall and Legitimate precision

Since the spam detection involves two sorts of emails (legitimate emails and spam), these two measurements are corresponding to the spam recall and spam precision. The formulas can be deduced accordingly.

4) Accuracy

Accuracy can reflect the whole performance of a spam filtering system. It can measure out the rate of emails categorized correctly by the system, including spam and legitimate emails. It is defined as follows.

$$A = \frac{n_{l\to l} + n_{s\to s}}{n_l + n_s} \tag{1.6}$$

where $n_{l\to l}$ means the number of legitimate emails correctly categorized while n_l and n_s means the total number of legitimate emails and spam, respectively.

5) Weighted Accuracy

Researchers found that the loss of legitimate emails (incorrectly be filtered out by the system) means people will miss important information in life, which may cause more severe consequence than spam being incorrectly categorized. In order to reflect the importance of legitimate emails, researchers defined the following formula as the way to calculate the weighted accuracy on the basis of accuracy.

$$A = \frac{\lambda n_{l\to l} + n_{s\to s}}{\lambda n_l + n_s} \tag{1.7}$$

where λ is the parameter reflecting the importance of legitimate emails.

The larger its value is, the more important the legitimate email is in the current case. Its value can be 9, 99, or 999. If it is defined as 999, it means the legitimate email is extremely important in such cases. When its value is 1, the weighted accuracy is equal to the accuracy directly.

6) F_β Measure

Spam recall and precision can only reflect one aspect of the spam filtering system, respectively, while one of the two measurements can not reflect the whole performance of the system. In order to solve this problem, F_β measure is viewed as combination of the two measurements and is defined as follows.

$$F_\beta = (1+\beta^2)\frac{R_s P_s}{\beta^2 P_s + R_s}. \tag{1.8}$$

where β represents the weighted accuracy reflecting the importance of precision compared with recall. In most cases, the value of β is 1, and then it is referred to as F_1 measure.

1.5.2 Standard Corpora

In 2000, Androutsopoulos et al. disposed and publicized LingSpam dataset [11]. This dataset is one of the classic datasets which were publicized earliest:

LingSpam: The dataset contains 2983 emails including 2412 legitimate emails. The percentage of spam is 16.63%. The emails involved in this dataset were all processed in advance. Information in the header of emails was all eliminated (except subject). The mark of html was also been eliminated. But the deficit of this dataset is that most of the emails are on linguistics which means using this dataset to evaluate spam detection system could bring about an over optimistic estimate.

In 2004, Androusopoulos et al. [13] collected, disposed and publicized classic datasets of PU series, which are now being widely used to evaluate various spam filtering systems. PU series contain four individual datasets below.

PU1: It contains 1099 emails, of which 481 are spam. All emails are normally-written English emails. Legitimate emails were collected in 36 months by the author firstly referred and spam emails were collected by him in later 22 months.

PU2: It contains 721 emails, of which 142 are spam. Similar to PU1, emails in this dataset are also in English. One of the colleagues of the author firstly referred collected these emails in 22 months.

PU3: It contains 4139 emails, of which 1826 are spam. Contrast to PU1 and PU2, this dataset covers emails both in English and in other languages. Legitimate emails in this dataset were collected by the second author while spam were cited from other datasets.

PUA: This one contains 1142 emails, 572 of which were spam. Like PU3, this dataset contains some emails in other languages and spam were from other datasets. Legitimate emails were collected by another colleague.

Medlock [130] disposed and publicized another large-scale email dataset called GenSpam.

GenSpam: It was composed of three parts. Part one is dataset for training including 8018 legitimate emails and 31235 spam. Part two is dataset for testing including 754 legitimate emails and 797 spam emails. Part three is dataset for self-adaption including 300 spam and 300 legitimate emails, which are used to detect the dynamic and self-adaption features of spam filtering systems.

Dataset ZH1 is a Chinese email dataset [241]. Chinese words in the emails have been separated. After such processing, the words were reflected as integer so as to protect email users' privacy.

ZH1: This dataset contains 1633 emails, of which 433 are legitimate emails and the percentage of spam is 73.79%. The average length of legitimate emails covers 819.06 words. The average length of spam covers 819.06 words. The shortest spam is 819.06 words long while the longest is 32810 words long.

1.6 Summary

In the current anti-spam techniques, intelligent spam detection methods are the most effective and promising approaches. Nevertheless, legal means and simple techniques can also play a role on some spam conforming to the defined characteristics, while it is difficult for the email protocol methods to be put into practice due to the high cost.

Feature extraction approach is the core part of an intelligent spam detection system, which plays a decisive role on the performance of classification. The research on newly proposed and improved feature extraction approaches will greatly promote the development of anti-spam technologies. The intelligent spam detection is wholly a new type of anti-spam techniques developed on the basis of the traditional simple anti-spam techniques. Currently, machine learning methods are widely used in the field of intelligent anti-spam and achieve high performance. Research on machine learning methods, espe-

cially classification techniques, and their application in spam filtering has a bright prospect in future development.

2

Artificial Immune System

CONTENTS

Artificial Immune System (AIS) is an inter-discipline research area that aims to build computational intelligence models by taking inspiration from Biological Immune System (BIS). This chapter first gives some knowledge of BIS and briefly introduces the origin and developments of AIS. Then, several AIS models are described in detail. Afterward, this chapter summarizes the main features and applications of AIS. Finally, the AIS-based anti-spam is presented and detailed.

2.1 Introduction

People have a keen interest on the biosphere since ancient times and have gotten inspiration from the structures and functions of biological systems and their regulatory mechanisms continuously. Since mid-20th century, researchers have focused on the simulation of the biological systems, especially the structures and functions of human beings. For examples, artificial neural network is to simulate the structure of the nerve system of human brain, fuzzy control is very similar to the fuzzy thinking and inaccurate reasoning of human be-

ings, and evolutionary computation algorithms are the direct simulations of the evolved processes of natural creatures.

In recent years, biological immune system has become an emerging bioinformatics research area. The immune system is a complex system consisting of organs, cells and molecules. The immune system is able to recognize the stimulation of "self" and "non-self", make a precise response, and retain the memory. It turns out from many researches that the immune system is of a variety of functions such as pattern recognition, learning, memory acquisition, diversity, fault-tolerant, distributed detection and so on.

These attractive properties of the biological immune system have drawn extensive attention of engineering researchers who have proposed many novel algorithms and techniques based on those principles of immunology. After introducing the concept of immunity, many researches in engineering have obtained more and more promising results, such as computer network security, intelligent robots, intelligent control and pattern recognition and fault diagnosis. These researches and applications not only can help us to further understand the immune system itself, but also to re-examine and solve practical engineering problems from the perspective of information processing way in biological immune system.

Building a computer security system in principle of the immune system opens a new research field of information security. Many structure, functions and mechanisms of the immune system are very helpful and referential to the research of computer security, such as antibody diversity, dynamic coverage and distribution. We believe that the excellent features of the immune system are the roots and original springs for us to build perfect computer security systems.

2.2 Biological Immune System

2.2.1 Overview

Biological immune system (BIS) is a highly complex, distributed, and paralleled natural system with multiple levels, which can identify the "self", exclude the "non-self", for maintaining the security and stability in the biological environment. It makes use of the innate immunity and adaptive immunity to generate accurate immune response against the invading antigens outside. BIS is robust to noise, distributed, self-organized, non-central control and having enhanced memory [37]. The original substance in an organism is called as "self" such as normal cells. The non-original substance in the organism is called as "non-self" like the invading antigens.

BIS consists of innate immunity (also known as non-specific immune) system and adaptive immunity (also known as specific immune) system. The two

Bibliography

[1] A. Abi-Haidar and L. Rocha. Adaptive spam detection inspired by a cross-regulation model of immune dynamics: A study of concept drift. *Artificial Immune Systems*, pages 36–47, 2008.

[2] U. Aickelin and S. Cayzer. The danger theory and its application to artificial immune systems. In *Proceedings of the First International Conference on Artificial Immune Systems*, pages 141–148, 2002.

[3] Uwe Aickelin, Peter Bentley, Steve Cayzer, Jungwon Kim, and Julie McLeod. Danger theory: The link between ais and ids? In *Artificial Immune Systems*, pages 147–155. Springer, 2003.

[4] Uwe Aickelin and Steve Cayzer. The danger theory and its application to artificial immune systems. *arXiv preprint arXiv:0801.3549*, 2008.

[5] Uwe Aickelin and Julie Greensmith. Sensing danger: Innate immunology for intrusion detection. *Information Security Technical Report*, 12(4):218–227, 2007.

[6] O. Al-Jarrah, I. Khater, and B. Al-Duwairi. Identifying potentially useful email header features for email spam filtering. In *ICDS 2012, The Sixth International Conference on Digital Society*, pages 140–145, 2012.

[7] O. Amayri and N. Bouguila. Online spam filtering using support vector machines. In *Computers and Communications, 2009. ISCC 2009. IEEE Symposium on*, pages 337–340. IEEE, 2009.

[8] D.S. Anderson, C. Fleizach, S. Savage, and G.M. Voelker. Spamscatter: Characterizing internet scam hosting infrastructure. In *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium*, pages 1–10. USENIX Association, 2007.

[9] Janecek Andreas and Ying Tan. Swarm intelligence for non-negative matrix factorization. *International Journal of Swarm Intelligence Research*, 2(4):12–34, 2011.

[10] Janecek Andreas and Ying Tan. Efficient euclidean distance transform algorithm of binary images in arbitrary dimensions. *Pattern Recognition*, 46(1):230–242, 2013.

[11] I. Androutsopoulos, J. Koutsias, K.V. Chandrinos, G. Paliouras, and C.D. Spyropoulos. An evaluation of naive bayesian anti-spam filtering. In *11th European Conference on Machine Learning (ECML 2000)*, pages 9–17. Barcelona, Spain, 2000.

[12] I. Androutsopoulos, G. Paliouras, V. Karkaletsis, G. Sakkis, C.D. Spyropoulos, and P. Stamatopoulos. Learning to filter spam e-mail: A comparison of a naive bayesian and a memory-based approach. In *4th European Conference on Principles and Practice of Knowledge Discovery in Databases*, pages 1–13. Lyon, France, 2000.

[13] I. Androutsopoulos, G. Paliouras, and E. Michelakis. Learning to filter unsolicited commercial e-mail. Technical report, DEMOKRITOS, National Center for Scientific Research, 2004.

[14] Ion Androutsopoulos, John Koutsias, Konstantinos V Chandrinos, and Constantine D Spyropoulos. An experimental comparison of naive bayesian and keyword-based anti-spam filtering with personal e-mail messages. In *Proceedings of the 23rd annual international ACM SIGIR conference on Research and development in information retrieval*, pages 160–167. ACM, 2000.

[15] H.B. Aradhye, G.K. Myers, and J.A. Herson. Image analysis for efficient categorization of image-based spam e-mail. In *Document Analysis and Recognition, 2005. Proceedings. Eighth International Conference on*, pages 914–918. IEEE, 2005.

[16] A. Attar, R.M. Rad, and R.E. Atani. A survey of image spamming and filtering techniques. *Artificial Intelligence Review*, pages 1–35, 2011.

[17] S. Balachandran, D. Dasgupta, F. Nino, and D. Garrett. A framework for evolving multi-shaped detectors in negative selection. In *Foundations of Computational Intelligence, 2007. FOCI 2007. IEEE Symposium on*, pages 401–408. IEEE, 2007.

[18] J. Balthrop, F. Esponda, S. Forrest, and M. Glickman. Coverage and generalization in an artificial immune system. In *Proceedings of the Genetic and Evolutionary Computation Conference*, pages 3–10. Citeseer, 2002.

[19] Yoshua Bengio, Patrice Simard, and Paolo Frasconi. Learning long-term dependencies with gradient descent is difficult. *Neural Networks, IEEE Transactions on*, 5(2):157–166, 1994.

[20] D. J. Bernstein. Internet mail 2000. `http://cr.yp.to/im2000.html`, Accessed: 2012.

[21] George B Bezerra, Tiago V Barra, Hamilton M Ferreira, Helder Knidel, Leandro Nunes de Castro, and Fernando J Von Zuben. An immunological filter for spam. In *Artificial Immune Systems*, pages 446–458. Springer, 2006.

[22] Steffen Bickel and Tobias Scheffer. Dirichlet-enhanced spam filtering based on biased samples. *Advances in neural information processing systems*, 19:161, 2007.

[23] B. Biggio, G. Fumera, I. Pillai, and F. Roli. Image spam filtering using visual information. In *Image Analysis and Processing, 2007. ICIAP 2007. 14th International Conference on*, pages 105–110. IEEE, 2007.

[24] B. Biggio, G. Fumera, I. Pillai, and F. Roli. A survey and experimental evaluation of image spam filtering techniques. *Pattern Recognition Letters*, pages 1436–1446, 2011.

[25] Enrico Blanzieri and Anton Bryl. A survey of learning-based techniques of email spam filtering. *Artificial Intelligence Review*, 29(1):63–92, 2008.

[26] Léon Bottou and Vladimir Vapnik. Local learning algorithms. *Neural computation*, 4(6):888–900, 1992.

[27] P.O. Boykin and V.P. Roychowdhury. Leveraging social networks to fight spam. *Computer*, 38(4):61–68, 2005.

[28] J. Brownlee. Clonal selection algorithms. Technical report, Complex Intelligent Systems Laboratory (CIS), Centre for Information Technology Research (CITR), Faculty of Information and Communication Technologies (ICT), Swinburne University of Technology, Victoria, Australia, Technical Report ID: 070209A, 2007.

[29] FM Burnet. Clonal selection and after. *Theoretical Immunology*, pages 63–85, 1978.

[30] Sir Frank Macfarlane Burnet et al. *The clonal selection theory of acquired immunity*. Vanderbilt University Press Nashville, 1959.

[31] B. Byun, C.H. Lee, S. Webb, and C. Pu. A discriminative classifier learning approach to image modeling and spam image identification. In *Proc. 4th Conference on Email and Anti-Spam*. Citeseer, 2007.

[32] James Carpinter and Ray Hunt. Tightening the net: A review of current and next generation spam filtering tools. *Computers & security*, 25(8):566–578, 2006.

[33] X. Carreras and L. Marquez. Boosting trees for anti-spam email filtering. In *4th International Conference on Recent Advances in Natural Language Processing*, pages 1–8. Tzigov Chark, BG, 2001.

[34] Chih-Chung Chang and Chih-Jen Lin. Libsvm: a library for support vector machines. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 2(3):27, 2011.

[35] Rui Chao and Ying Tan. A virus detection system based on artificial immune system. In *Computational Intelligence and Security, 2009. CIS'09. International Conference on*, volume 1, pages 6–10. IEEE, 2009.

[36] Y. Chao, L. Yiwen, and L. Aolin. The danger sensed method by feature changes. *Energy Procedia*, 13:4429–4437, 2011.

[37] Mark Walport Charles A Janeway, Jr Paul Travers and Mark J Shlomchik. *Immunobiology: The Immune System in Health and Disease*. Number 2 in Immunobiology: The Immune System in Health and Disease. Garland Science, 2005.

[38] Haibin Cheng, Pang-Ning Tan, and Rong Jin. Localized support vector machine and its efficient algorithm. In *SDM*, pages 461–466. SIAM, 2007.

[39] Haibin Cheng, Pang-Ning Tan, and Rong Jin. Efficient algorithm for localized support vector machine. *Knowledge and Data Engineering, IEEE Transactions on*, 22(4):537–549, 2010.

[40] Ali Ciltik and Tunga Gungor. Time-efficient spam e-mail filtering using n-gram models. *Pattern Recognition Letters*, 29(1):19–33, 2008.

[41] J. Clark, I. Koprinska, and J. Poon. A neural network based approach to automated e-mail classification. In *Web Intelligence, 2003. WI 2003. Proceedings. IEEE/WIC International Conference on*, pages 702–705. IEEE, 2003.

[42] Irun R Cohen. Real and artificial immune systems: computing the state of the body. *Nature Reviews Immunology*, 7(7):569–574, 2007.

[43] W.W. COHEN. Fast effective rule induction. In *Proceedings of 12th Int. Conf.Machine Learning*, pages 115–123. San Mateo, CA: Morgan Kaufmann, 1995.

[44] Commtouch. Internet threats trend report-april 2012. Technical report, 2012.

[45] G.V. Cormack. Email spam filtering: A systematic review. *Foundations and Trends in Information Retrieval*, 1(4):335–455, 2007.

[46] Thomas Cover and Peter Hart. Nearest neighbor pattern classification. *Information Theory, IEEE Transactions on*, 13(1):21–27, 1967.

[47] L.F. Cranor and B.A. LaMacchia. Spam! *Communications of the ACM*, 41(8):74–83, 1998.

[48] M. Crispin. Rfc2060: Internet message access protocol - version 4rev1. `http://www.ietf.org/rfc/rfc2060.txt`, Accessed: 2012.

[49] N. Cruz-Cortés, D. Trejo-Pérez, and C. Coello. Handling constraints in global optimization using an artificial immune system. *Artificial Immune Systems*, pages 234–247, 2005.

[50] V. Cutello and G. Nicosia. Multiple learning using immune algorithms. In *Proceedings of 4th International Conference on Recent Advances in Soft Computing, RASC*, pages 102–107, 2002.

[51] D. Dasgupta and F. González. An immunity-based technique to characterize intrusions in computer networks. *Evolutionary Computation, IEEE Transactions on*, 6(3):281–291, 2002.

[52] D. Dasgupta, S. Yu, and N. Majumdar. Milamultilevel immune learning algorithm. In *Genetic and Evolutionary ComputationGECCO 2003*, pages 183–194. Springer, 2003.

[53] D. Dasgupta, S. Yu, and F. Nino. Recent advances in artificial immune systems: Models and applications. *Applied Soft Computing*, 11(2):1574–1587, 2011.

[54] Dipankar Dasgupta. Advances in artificial immune systems. *Computational Intelligence Magazine, IEEE*, 1(4):40–49, 2006.

[55] Dipankar Dasgupta and Nii Attoh-Okine. Immunity-based systems: A survey. In *Systems, Man, and Cybernetics, 1997. Computational Cybernetics and Simulation., 1997 IEEE International Conference on*, volume 1, pages 369–374. IEEE, 1997.

[56] L Nunes de Castro and Jon Timmis. An artificial immune network for multimodal function optimization. In *Evolutionary Computation, 2002. CEC'02. Proceedings of the 2002 Congress on*, volume 1, pages 699–704. IEEE, 2002.

[57] Leandro Nunes De Castro and Jonathan Timmis. *Artificial immune systems: a new computational intelligence approach*. Springer, 2002.

[58] Leandro Nunes De Castro and Fernando José Von Zuben. Artificial immune systems: Part i–basic theory and applications. *Universidade Estadual de Campinas, Dezembro de, Tech. Rep*, 210, 1999.

[59] L.N. De Castro and F.J. Von Zuben. The clonal selection algorithm with engineering applications. In *Proceedings of GECCO*, volume 2000, pages 36–39, 2000.

[60] L.N. de Castro and F.J. Von Zuben. ainet: An artificial immune network for data analysis. *Data Mining: A Heuristic Approach*, 1:231–259, 2001.

[61] L.N. De Castro and F.J. Von Zuben. Learning and optimization using the clonal selection principle. *Evolutionary Computation, IEEE Transactions on*, 6(3):239–251, 2002.

[62] P.A.D. de Castro and F.J. Von Zuben. Bais: A bayesian artificial immune system for the effective handling of building blocks. *Information Sciences*, 179(10):1426–1440, 2009.

[63] D. DeBarr and H. Wechsler. Using social network analysis for spam detection. *Advances in Social Computing*, pages 62–69, 2010.

[64] C. Domeniconi and D. Gunopulos. Incremental support vector machine construction. In *Proc. IEEE International Conference on Data Mining (ICDM'01)*, pages 589–592, San Jose, CA, USA, December 2001.

[65] M. Dredze, R. Gevaryahu, and A. Elias-Bachrach. Learning fast classifiers for image spam. In *Proceedings of the Conference on Email and Anti-Spam (CEAS)*, 2007.

[66] H. Drucker, C. J. C. Burges, L. Kauffman, A. Smola, and V. N. Vapnik. Support vector regression machines. In Michael C. Mozer, Michael I. Jordan, and Thomas Petsche, editors, *Advances in Neural Information Processing System (NIPS)*, volume 9, pages 155–161. MIT Press, Cambridge, MA, 1997.

[67] Harris Drucker, S Wu, and Vladimir N Vapnik. Support vector machines for spam categorization. *Neural Networks, IEEE Transactions on*, 10(5):1048–1054, 1999.

[68] Z. Duan, Y. Dong, and K. Gopalan. Dmtp: Controlling spam through message delivery differentiation. *Computer Networks*, 51(10):2616–2630, 2007.

[69] Z. Duan, K. Gopalan, and X. Yuan. An empirical study of behavioral characteristics of spammers: Findings and implications. *Computer Communications*, 34:1764–1776, 2011.

[70] S. Forrest, A.S. Perelson, L. Allen, and R. Cherukuri. Self-nonself discrimination in a computer. In *Research in Security and Privacy, 1994. Proceedings., 1994 IEEE Computer Society Symposium on*, pages 202–212. IEEE, 1994.

[71] Alex Alves Freitas and Jonathan Timmis. Revisiting the foundations of artificial immune systems for data mining. *Evolutionary Computation, IEEE Transactions on*, 11(4):521–540, 2007.

[72] G. Fumera, I. Pillai, and F. Roli. Spam filtering based on the analysis of text information embedded into images. *The Journal of Machine Learning Research*, 7:2699–2720, 2006.

[73] J.C. Galeano, A. Veloza-Suan, and F.A. González. A comparative analysis of artificial immune network models. In *Proceedings of the 2005 Conference on Genetic and Evolutionary Computation*, pages 361–368. ACM, 2005.

[74] Wilfried Gansterer, Michael Ilger, Peter Lechner, Richard Neumayer, and Jürgen Strauß. Anti-spam methods - state of the art. *Institute of Distributed and Multimedia Systems, University of Vienna*, 2005.

[75] Y. Gao, A. Choudhary, and G. Hua. A comprehensive approach to image spam detection: From server to client solution. *IEEE Transactions on Information Forensics and Security*, 5(4):826–836, 2010.

[76] Y. Gao, M. Yang, X. Zhao, B. Pardo, Y. Wu, T.N. Pappas, and A. Choudhary. Image spam hunter. In *Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on*, pages 1765–1768. IEEE, 2008.

[77] Yang Gao, Guyue Mi, and Ying Tan. An adaptive concentraton selection model for spam detection. In *The Fifth International Conference on Swarm Intelligence (ICSI 2014)*, pages 223–233. Springer, 2014.

[78] S. Garrett. A paratope is not an epitope: Implications for immune network models and clonal selection. *Artificial Immune Systems*, pages 217–228, 2003.

[79] F. González, D. Dasgupta, and J. Gómez. The effect of binary matching rules in negative selection. In *Genetic and Evolutionary ComputationGECCO 2003*, pages 195–206. Springer, 2003.

[80] Alex Graves. *Supervised sequence labelling with recurrent neural networks*, volume 385. Springer, 2012.

[81] G.A. Grimes. Compliance with the can-spam act of 2003. *Communications of the ACM*, 50(2):56–62, 2007.

[82] Suicheng Gu, Ying Tan, and Xingui He. Discriminant analysis via support vectors. *Neurocomputing*, 73(10-12):1669–1675, 2010.

[83] Suicheng Gu, Ying Tan, and Xingui He. Laplacian smoothing transform for face recognition. *Science China (Information Science)*, 53(12):2415–2428, 2010.

[84] Suicheng Gu, Ying Tan, and Xingui He. Laplacian smoothing transform for face recognition. *Science China (Information Science)*, 53(12):24150–2428, 2010.

[85] Suicheng Gu, Ying Tan, and Xingui He. Recent-biased learning for time series forecast. *Information Science*, 237(10):29–38, 2013.

[86] Zhenghuo Guo, Zhengkai Liu, and Ying Tan. Detector generating algorithm based on hyper-sphere. *Journal of Chinese Computer Systems*, 26(12):1641–1645, 2005.

[87] Zhenhe Guo, Zhengkai Liu, and Ying Tan. An nn-based malicious executables detection algorithm based on immune principles. In *Advances in Neural Networks-ISNN 2004*, pages 675–680. Springer, 2004.

[88] Thiago S Guzella and Walmir M Caminhas. A review of machine learning approaches to spam filtering. *Expert Systems with Applications*, 36(7):10206–10222, 2009.

[89] Thiago S Guzella, Tomaz A Mota-Santos, Joaquim Quinteiro Uchôa, and Walmir M Caminhas. Identification of spam messages using an approach inspired on the immune system. *Biosystems*, 92(3):215–225, 2008.

[90] Mark Hall, Eibe Frank, Geoffrey Holmes, Bernhard Pfahringer, Peter Reutemann, and Ian H Witten. The weka data mining software: an update. *ACM SIGKDD explorations newsletter*, 11(1):10–18, 2009.

[91] J. He and B. Thiesson. Asymmetric gradient boosting with application to spam filtering. In *Proceedings of Fourth Conference on Email and Anti-Spam CEAS*, pages 1–8. California, USA, 2007.

[92] P. He, X. Wen, and W. Zheng. A simple method for filtering image spam. In *Computer and Information Science, 2009. ICIS 2009. Eighth IEEE/ACIS International Conference on*, pages 910–913. IEEE, 2009.

[93] S. Heron. Technologies for spam detection. *Network Security*, 2009(1):11–15, 2009.

[94] S. Hershkop. *Behavior-based email analysis with application to spam detection*. PhD thesis, Columbia University, 2006.

[95] Sepp Hochreiter. Untersuchungen zu dynamischen neuronalen netzen. *Master's thesis, Institut fur Informatik, Technische Universitat, Munchen*, 1991.

[96] Sepp Hochreiter and Jürgen Schmidhuber. Long short-term memory. *Neural computation*, 9(8):1735–1780, 1997.

[97] S. A. Hofmeyr and S. Forrest. Architecture for an artificial immune system. *Evolutionary Computation*, 8(4):443–473, 2000.

[98] F. Huamin, Y. Xinghua, L. Biao, and J. Chao. A spam filtering method based on multi-modal features fusion. In *Computational Intelligence and Security (CIS), 2011 Seventh International Conference on*, pages 421–426. IEEE, 2011.

[99] Xi Huang, Ying Tan, and Xingui He. An intelligent multi-feature statistical approach for discrimination of driving conditions of hybrid electric vehicle. *IEEE Transactions on Intelligent Transportation Systems*, 12(2):453–465, 2011.

[100] J Hunt, J Timmis, D Cooke, et al. Jisys: Development of an artificial immune system for real world applicaitions, artificial immune systems and their applications, 1998.

[101] J.E. Hunt and D.E. Cooke. Learning using an artificial immune system. *Journal of Network and Computer Applications*, 19(2):189–212, 1996.

[102] J. Ioannidis. Fighting spam by encapsulating policy in email addresses. In *Proceedings of NDSS*, pages 1–8, 2003.

[103] Andreas Janecek and Ying Tan. Iterative improvement of the multiplicative update nmf algorithm using nature-inspired optimization. In *Natural Computation (ICNC), 2011 Seventh International Conference on*, volume 3, pages 1668–1672. IEEE, 2011.

[104] N.K. Jerne. Towards a network theory of the immune system. In *Annales D'Immunologie*, volume 125, pages 373–389, 1974.

[105] Z. Ji and D. Dasgupta. Real-valued negative selection algorithm with variable-sized detectors. In *Genetic and Evolutionary Computation–GECCO 2004*, pages 287–298. Springer, 2004.

[106] Z. Ji and D. Dasgupta. Revisiting negative selection algorithms. *Evolutionary Computation*, 15(2):223–251, 2007.

[107] Licheng Jiao and Haifeng Du. Development and prospect of the artificial immune system. in chinese. *ACTA ELECTRONICA SINICA*, 31(10):1540–1548, 2003.

[108] Xiyu Liu Jun Wang and Xin Wang. Artificial immune system and analysis of its models. in chinese. *Computer Technology and Development*, 16(7):105–107, 2006.

[109] Ioannis Kanaris, Konstantinos Kanaris, Ioannis Houvardas, and Efstathios Stamatatos. Words versus character n-grams for anti-spam filtering. *International Journal on Artificial Intelligence Tools*, 16(06):1047–1067, 2007.

[110] Vojislav Kecman and J Paul Brooks. Locally linear support vector machines and other local models. In *Neural Networks (IJCNN), The 2010 International Joint Conference on*, pages 1–6. IEEE, 2010.

[111] J. Klensin. Rfc2821: Simple mail transfer protocol. `http://www.ietf.org/rfc/rfc2821.txt`, Accessed: 2012.

[112] M. Kokkodis and M. Faloutsos. Spamming botnets: Are we losing the war. In *The 6th Conference on Email and Anti-Spam (CEAS)*, pages 1–3. Mountain View, California USA, 2009.

[113] Irena Koprinska, Josiah Poon, James Clark, and Jason Chan. Learning to classify e-mail. *Information Sciences*, 177(10):2167–2187, 2007.

[114] SB Kotsiantis. Supervised machine learning: A review of classification techniques. *Informatica*, 31:249–268, 2007.

[115] S. Krasser, Y. Tang, J. Gould, D. Alperovitch, and P. Judge. Identifying image spam based on header and file properties using c4. 5 decision trees and support vector machine learning. In *Information Assurance and Security Workshop, 2007. IAW'07. IEEE SMC*, pages 255–261. IEEE, 2007.

[116] H.Y. Lam and D.Y. Yeung. A learning approach to spam detection based on social networks. In *Proceedings of Fourth Conference on Email and Anti-Spam*, pages 1–9. California USA, 2007.

[117] Yuchun Lee. Handwritten digit recognition using k nearest-neighbor, radial-basis function, and backpropagation neural networks. *Neural computation*, 3(3):440–449, 1991.

[118] F. Li and M.H. Hsieh. An empirical study of clustering behavior of spammers and group-based anti-spam strategies. In *CEAS 2006: Proceedings of the 3rd Conference on Email and Anti-Spam*, 2006.

[119] P. Li, H. Yan, G. Cui, and Y. Du. Integration of local and global features for image spam filtering. *Journal of Computational Information Systems*, 8(2):779–789, 2012.

[120] Yang Li, Binxing Fang, Li Guo, and Shen Wang. Research of a novel anti-spam technique based on users's feedback and improved naive bayesian approach. In *Networking and Services, 2006. ICNS'06. International conference on*, pages 86–86. IEEE, 2006.

[121] Z. Li and H. Shen. Soap: A social network aided personalized and effective spam filter to clean your e-mail box. In *INFOCOM, 2011 Proceedings IEEE*, pages 1835–1843. IEEE, 2011.

[122] Z. Li, Y. Zhang, and H.Z. Tan. An efficient artificial immune network with elite-learning. In *Natural Computation, 2007. ICNC 2007. Third International Conference on*, volume 4, pages 213–217. IEEE, 2007.

[123] Q. Liu, Z. Qin, H. Cheng, and M. Wan. Efficient modeling of spam images. In *Intelligent Information Technology and Security Informatics (IITSI), 2010 Third International Symposium on*, pages 663–666. IEEE, 2010.

[124] Q. Luo, B. Liu, J. Yan, and Z. He. Research of a spam filtering algorithm based on naive bayes and ais. In *Computational and Information Sciences (ICCIS), 2010 International Conference on*, pages 152–155. IEEE, 2010.

[125] Wenjian Luo, Ying Tan, and Xufa Wang. A novel negative selection algorithm with an array of partial matching lengths for each detector. In *PPSN 2006*, pages 112–121. Springer, 2006.

[126] W. Ma, D. Tran, and D. Sharma. A novel spam email detection system based on negative selection. In *Computer Sciences and Convergence Information Technology, 2009. ICCIT'09. Fourth International Conference on*, pages 987–992. IEEE, 2009.

[127] M.N. Marsono. *Towards improving e-mail content classification for spam control: Architecture, abstraction, and strategies*. PhD thesis, University of Victoria, 2007.

[128] Polly Matzinger. Essay 1: the danger model in its historical context. *Scandinavian journal of immunology*, 54(1-2):4–9, 2001.

[129] Polly Matzinger. The danger model: a renewed sense of self. *Science*, 296(5566):301–305, 2002.

[130] Ben Medlock. An adaptive, semi-structured language model approach to spam filtering on a new corpus. In *CEAS*, 2006.

[131] B. Mehta, S. Nangia, M. Gupta, and W. Nejdl. Detecting image spam using visual features and near duplicate detection. In *Proceedings of the 17th International Conference on World Wide Web*, pages 497–506. ACM, 2008.

[132] Vangelis Metsis, Ion Androutsopoulos, and Georgios Paliouras. Spam filtering with naive bayes-which naive bayes? In *CEAS*, pages 27–28, 2006.

[133] Guyue Mi, Pengtao Zhang, and Ying Tan. Feature construction approach for email categorization based on term space partition. In *Neural Networks (IJCNN), The 2013 International Joint Conference on*, pages 1–8. IEEE, 2013.

[134] Guyue Mi, Pengtao Zhang, and Ying Tan. A multi-resolution-concentration based feature construction approach for spam filtering. In *Neural Networks (IJCNN), The 2013 International Joint Conference on*, pages 1–8. IEEE, 2013.

[135] P. Mitra, C. A. Murthy, and S. K. Pal. Data condensation in large databases by incremental learning with support vector machines. In *Proc. IEEE International Conference on Pattern Recognition*, volume 2, pages 708–711, September 2000.

[136] Hongwei Mo and Hongzhang Jin. Application of artificial immune system to computer security. in chinese. *Journal of Harbin Engineering University*, 24(3):278–282, 2003.

[137] J. Myers and M. Rose. Rfc1939: Post office protocol - version3. `http://www.ietf.org/rfc/rfc1939.txt`, Accessed: 2012.

[138] O. Nasaroui, F. Gonzalez, and D. Dasgupta. The fuzzy artificial immune system: Motivations, basic concepts, and application to clustering and web profiling. In *Fuzzy Systems, 2002. FUZZ-IEEE'02. Proceedings of the 2002 IEEE International Conference on*, volume 1, pages 711–716. IEEE, 2002.

[139] M. Neal. An artificial immune system for continuous analysis of time-varying data. In *Proceedings of the 1st International Conference on Artificial Immune Systems (ICARIS)*, volume 1, pages 76–85, 2002.

[140] Terri Oda and Tony White. Developing an immunity to spam. In *Genetic and Evolutionary ComputationGECCO 2003*, pages 231–242. Springer, 2003.

[141] Terri Oda and Tony White. Immunity from spam: An analysis of an artificial immune system for junk email detection. In *Artificial Immune Systems*, pages 276–289. Springer, 2005.

[142] White T. Oda T. Spam detection using an artificial immune system. *Crossroads Magazine*, 2004.

[143] Bill on Telecommunication. Tkg 2003. Technical report, Accessed: 2009.

[144] E. Osuna, R. Freund, and F. Girosi. An improved training algorithm for support vector machines. In *Proc. IEEE Workshop on Neural Networks for Signal Processing (NNSP'97)*, pages 276–285, September 1997.

[145] J. C. Platt. Sequential minimal optimization: A fast algorithm for training support vector machines. In Bernhard Scholkopf, Christopher J. C. Burges, and Alexander J. Smola, editors, *Advances in Kernel Method: Support Vector Learning*, page 185C208. MIT Press, Cambridge, MA, 1998.

[146] J. B. Postel. Rfc821: Simple mail transfer protocol. `http://www.ietf.org/rfc/rfc0821.txt`, Accessed: 2012.

[147] C.E. Prieto, F. Nino, and G. Quintana. A goalkeeper strategy in robot soccer based on danger theory. In *Evolutionary Computation, 2008. CEC 2008.(IEEE World Congress on Computational Intelligence). IEEE Congress on*, pages 3443–3447. IEEE, 2008.

[148] J. Qing, R. Mao, R. Bie, and X.Z. Gao. An ais-based e-mail classification method. *Emerging Intelligent Computing Technology and Applications. With Aspects of Artificial Intelligence*, pages 492–499, 2009.

[149] J. Ross Quinlan. Induction of decision trees. *Machine learning*, 1(1):81–106, 1986.

[150] John Ross Quinlan. *C4. 5: programs for machine learning*, volume 1. Morgan kaufmann, 1993.

[151] A. Ramachandran and N. Feamster. Understanding the network-level behavior of spammers. In *ACM SIGCOMM Computer Communication Review*, volume 36, pages 291–302. ACM, 2006.

[152] A. Ramachandran, N. Feamster, and S. Vempala. Filtering spam with behavioral blacklisting. In *Proceedings of the 14th ACM Conference on Computer and Communications Security*, pages 342–351. ACM, 2007.

[153] A.V. Ramachandran. *Mitigating spam using network-level features*. PhD thesis, August 2011.

[154] Ferris Research. Spam, spammers, and spam conrol: A white paper by ferris research. Technical report, 2009.

[155] Guangchen Ruan and Ying Tan. Intelligent detection approaches for spam. In *Natural Computation, 2007. ICNC 2007. Third International Conference on*, volume 3, pages 672–676. IEEE, 2007.

[156] Guangchen Ruan and Ying Tan. A three-layer back-propagation neural network for spam detection using artificial immune concentration. *Soft Computing*, 14(2):139–150, 2010.

[157] Mehran Sahami, Susan Dumais, David Heckerman, and Eric Horvitz. A bayesian approach to filtering junk e-mail. In *Learning for Text Categorization: Papers from the 1998 workshop*, volume 62, pages 98–105, 1998.

[158] Georgios Sakkis, Ion Androutsopoulos, Georgios Paliouras, Vangelis Karkaletsis, Constantine D Spyropoulos, and Panagiotis Stamatopoulos. A memory-based approach to anti-spam filtering for mailing lists. *Information Retrieval*, 6(1):49–73, 2003.

[159] S. Salehi and A. Selamat. Hybrid simple artificial immune system (sais) and particle swarm optimization (pso) for spam detection. In *Software Engineering (MySEC), 2011 5th Malaysian Conference in*, pages 124–129. IEEE, 2011.

[160] E.P. Sanz, J.M. Gomez Hidalgo, and J.C. Cortizo Perez. Email spam filtering. *Advances in Computers*, 74:45–114, 2008.

[161] S. Sarafijanovic and J.Y. Le Boudec. Artificial immune system for collaborative spam filtering. *Nature Inspired Cooperative Strategies for Optimization (NICSO 2007)*, pages 39–51, 2008.

[162] Shinnou h. Sasaki M. Spam detection using text clustering. In *Proceedings of International Conference on Cyberworlds*, pages 316–319, 2005.

[163] Singer Y Schapire R E. Boostexter: A boosting-based system for text categorization. *Machine Learning*, 39(2):135–168, 2000.

[164] Singhal A Schapire R E, Singer Y. Boosting and rocchio applied to text filtering. In *Proceedings of 21st Annu. Int. Conf. Inform. Retrieval, SIGIR*, 1998.

[165] Karl-Michael Schneider. A comparison of event models for naive bayes anti-spam e-mail filtering. In *Proceedings of the tenth conference on European chapter of the Association for Computational Linguistics-Volume 1*, pages 307–314. Association for Computational Linguistics, 2003.

[166] D. Sculley. *Advances in online learning-based spam filtering*. PhD thesis, TUFTS UNIVERSITY, 2008.

[167] Andrew Secker, Alex A Freitas, and Jon Timmis. A danger theory inspired approach to web mining. In *Artificial Immune Systems*, pages 156–167. Springer, 2003.

[168] Andrew Secker, Alex Alves Freitas, and Jon Timmis. Aisec: an artificial immune system for e-mail classification. In *Evolutionary Computation, 2003. CEC'03. The 2003 Congress on*, volume 1, pages 131–138. IEEE, 2003.

[169] Richard Segal. Combining global and personal anti-spam filtering. In *CEAS*, 2007.

[170] Raju Shrestha and Yaping Lin. Improved bayesian spam filtering based on co-weighted multi-area information. In *Advances in Knowledge Discovery and Data Mining*, pages 650–660. Springer, 2005.

[171] C. Siefkes, F. Assis, S. Chhabra, and W. Yerazunis. Combining winnow and orthogonal sparse bigrams for incremental spam filtering. In *Knowledge Discovery in Databases: PKDD 2004*, pages 410–421. Springer, 2004.

[172] Burim Sirisanyalak and Ohm Sornil. An artificial immunity-based spam detection system. In *Evolutionary Computation, 2007. CEC 2007. IEEE Congress on*, pages 3392–3398. IEEE, 2007.

[173] Sophos. Security threat report 2012. Technical report, 2012.

[174] Anti spam Center of ISC. 2008 4q anti-spam investigation report. Technical report, Accessed: 2009.

[175] T. Subramaniam, H.A. Jalab, and A.Y. Taqa. Overview of textual antispam filtering techniques. *International Journal of the Physical Sciences*, 5(12):1869–1882, 2010.

[176] Zhiyong Sun and Wei Wei. Artificial immune system and its application. in chinese. *Computer Engineering*, 29(15), 2003.

[177] N. A. Syed, H. Liu, and K. K. Sung. Incremental learning with support vector machines. In *Proc. International Joint Conference on Artificial Intelligence (IJCAI'99)*, Stockholm, Sweden, 1999.

[178] Symantec. Symantec intelligence report: January 2012. Technical report, 2012.

[179] Mail Abuse Prevention Systems. Definition of spam. `http://www.mail-abuse.com`, Accessed: 2012.

[180] Joachims T. A probabilistic analysis of the rocchio algorithm with tfidf for text categorization. In *Proceedings of 14th Int. Conf. Machine Learning*. CA: Morgan Kaufman, 1997.

[181] Nicholas T. Using adaboost and decision stumps to identify spam e-mail. Technical report, Accessed: 2009.

[182] Y. Tan. Particle swarm optimization algorithms inspired by immunity-clonal mechanism and their applications to spam detection. *International Journal of Swarm Intelligence Research (IJSIR)*, 1(1):64–86, 2010.

[183] Y. Tan and J. Wang. Nonlinear blind separation using higher-order statistics and a genetic algorithm. *IEEE Transaction on Evolutionary Computation*, 5(6):600–612, 2001.

[184] Y Tan and ZM Xiao. Clonal particle swarm optimization and its applications. In *Evolutionary Computation, 2007. CEC 2007. IEEE Congress on*, pages 2303–2309. IEEE, 2007.

[185] Ying Tan. Swarm robotics: Collective behavior inspired by nature. *Journal of Comput Sci Syst Biol (JCSB)*.

[186] Ying Tan. Neural network design approach of cosine-modulated fir filter bank and compactly supported wavelets with almost pr property. *Signal Processing*, 69(1):29–48, 1998.

[187] Ying Tan. Editorial: Special issue on advances in swarm intelligence for neural networks. *Neurocomputing*, 148(1):1–2, 2014.

[188] Ying Tan. *Fireworks algorithms: a swarm intelligence optimization method*. Springer, 2015.

[189] Ying Tan. *Introduction to Fireworks algorithms*. China Science Press, 2015.

[190] Ying Tan and Chao Deng. Solving for a quadratic programming with a quadratic constraint based on a neural network frame. *Neurocomputing*, 30:117–128, 2000.

[191] Ying Tan, Chao Deng, and Guangchen Ruan. Concentration based feature construction approach for spam detection. In *Neural Networks, 2009. IJCNN 2009. International Joint Conference on*, pages 3088–3093. IEEE, 2009.

[192] Ying Tan and Zhenhe Guo. Algorithms of non-self detector by negative selection principle in artificial immune system. In *Advances in Natural Computation*, pages 867–875. Springer, 2005.

[193] Ying Tan and Zhengkai Liu. On matrix eigendecomposition by neural networks. *Neural Network World,International Journal on Neural and Mass-Parallel Computing and Information Systems*, 8(3):337–352, 1998.

[194] Ying Tan, Guyue Mi, Yuanchun Zhu, and Chao Deng. Artificial immune system based methods for spam filtering. In *2013 IEEE International Symposium on Circuits and Systems (ISCAS 2013)*, pages 2484–2488. IEEE, 2013.

[195] Ying Tan and Guangchen Ruan. Uninterrupted approaches for spam detection based on svm and ais. *International Journal of Computational Intelligence*, 1(1):1–26, 2014.

[196] Ying Tan and Jun Wang. A support vector machine with a hybrid kernel and minimal vapnik-chervonenkis dimension. *Knowledge and Data Engineering, IEEE Transactions on*, 16(4):385–395, 2004.

[197] Ying Tan and Jun Wang. A support vector network with hybrid kernel and minimal vapnik-chervonenkis dimension. *IEEE Trans. On Knowledge and Data Engineering*, 26(2):385–395, 2004.

[198] Ying Tan and Jun Wang. Recent advances in finger vein based biometrics techniques. *CAAI Transactions on Intelligent Systems*, 6(6):471–482, 2011.

[199] Ying Tan, Jun Wang, and Zurada JM. Nonlinear blind source separation using radial basis function networks. *IEEE Transaction on Neural Networks*, 12(1):124–134, 2001.

[200] Ying Tan and Yuanchun Zhu. Advances in anti-spam techniques. *CAAI Transactions on Intelligent Systems*, 5(3):189–201, 2010.

[201] Ying Tan and Yuanchun Zhu. Fireworks algorithm for optimization. In *Advances in Swarm Intelligence*, pages 355–364. Springer, 2010.

[202] J. Timmis. *Artificial immune systems: A novel data analysis technique inspired by the immune network theory.* PhD thesis, Department of Computer Science, 2000.

[203] J. Timmis, A. Hone, T. Stibor, and E. Clark. Theoretical advances in artificial immune systems. *Theoretical Computer Science*, 403(1):11–32, 2008.

[204] J. Timmis and M. Neal. A resource limited artificial immune system for data analysis. *Knowledge-Based Systems*, 14(3):121–130, 2001.

[205] Jon Timmis. Artificial immune systems - today and tomorrow. *Natural computing*, 6(1):1–18, 2007.

[206] Jonathan Timmis, P Andrews, N Owens, and Edward Clark. An interdisciplinary perspective on artificial immune systems. *Evolutionary Intelligence*, 1(1):5–26, 2008.

[207] L.S. Tseng and C.H. Wu. Detection of spain e-mails by analyzing the distributing behaviors of e-mail servers. In *Design and Application of Hybrid Intelligent Systems*, pages 1024–1033. IOS Press, 2003.

[208] M. Uemura and T. Tabata. Design and evaluation of a bayesian-filter-based image spam filtering method. In *Information Security and Assurance, 2008. ISA 2008. International Conference on*, pages 46–51. IEEE, 2008.

[209] Carnegie Mellon University. Completely automated public turing test to tell computers and humans apart. `http://www.captcha.net/`, Accessed: 2012.

[210] Vladimir Vapnik. *The nature of statistical learning theory.* springer, 2000.

[211] Vladimir Naumovich Vapnik and Samuel Kotz. *Estimation of dependences based on empirical data*, volume 40. Springer-Verlag New York, 1982.

[212] V.N. Vapnik. Principles of risk minimization for learning theory. In *Advances in Neural Information Processing Systems*, volume 4, pages 831–838, 1992.

[213] L. von Ahn, M. Blum, and J. Langford. Telling humans and computers apart automatically. *Communications of the ACM*, 47(2):56–60, February 2004.

[214] M. Wan, F. Zhang, H. Cheng, and Q. Liu. Text localization in spam image using edge features. In *Communications, Circuits and Systems, 2008. ICCCAS 2008. International Conference on*, pages 838–842. IEEE, 2008.

[215] C. Wang, F. Zhang, F. Li, and Q. Liu. Image spam classification based on low-level image features. In *Communications, Circuits and Systems (ICCCAS), 2010 International Conference on*, pages 290–293. IEEE, 2010.

[216] Feng Wang, Zhisheng You, and Lichun Man. Immune-based peer-to-peer model for anti-spam. In *Computational Intelligence and Bioinformatics*, pages 660–671. Springer, 2006.

[217] L. Wang, S. Ma, and X. Hei. Research on an immune mechanism based intelligent spam filter. In *Computer Science and Software Engineering, 2008 International Conference on*, volume 3, pages 673–676. IEEE, 2008.

[218] W. Wang, S. Gao, and Z. Tang. A complex artificial immune system. In *Natural Computation, 2008. ICNC'08. Fourth International Conference on*, volume 6, pages 597–601. IEEE, 2008.

[219] Wei Wang, Peng-tao Zhang, Ying Tan, and Xin-gui He. A feature extraction method of computer viruses based on artificial immune and code relevance. *Chinese Journal of Computer*, 34(2):204–215, 2011.

[220] Wei Wang, Peng-tao Zhang, Ying Tan, and Xin-gui He. An immune local concentration based virus detection approach. *Journal of Zhejiang University SCIENCE C*, 12(6):443–454, 2011.

[221] Wei Wang, Pengtao Zhang, and Ying Tan. An immune concentration based virus detection approach using particle swarm optimization. In *Advances in Swarm Intelligence*, pages 347–354. Springer, 2010.

[222] Wei Wang, Pengtao Zhang, Ying Tan, and Xingui He. A hierarchical artificial immune model for virus detection. In *Computational Intelligence and Security, 2009. CIS'09. International Conference on*, volume 1, pages 1–5. IEEE, 2009.

[223] Z. Wang, W. Josephson, Q. Lv, M. Charikar, and K. Li. Filtering image spam with near-duplicate detection. In *Proceedings of CEAS*, 2007.

[224] A. Watkins, X. Bi, and A. Phadke. Parallelizing an immune-inspired algorithm for efficient pattern recognition. *Intelligent Engineering Systems through Artificial Neural Networks: Smart Engineering System Design: Neural Networks, Fuzzy Logic, Evolutionary Programming, Complex Systems and Artificial Life*, 13:225–230, 2003.

[225] B. Watson. Beyond identity: Addressing problems that persist in an electronic mail system with reliable sender identification. In *CEAS 2004: First Conference on Email and Anti-Spam*, pages 1–8. California, USA, 2004.

[226] Guyue Mi Wenrui He and Ying Tan. Parameter optimization of local-concentration model for spam detection by using fireworks algorithm. In *Proceedings of the fourth International Conferencce on Swarm Intelligence (ICSI 2013)*, pages 439–450, 2013.

[227] A.G. West, A.J. Aviv, J. Chang, and I. Lee. Mitigating spam using spatio-temporal reputation. Technical report, University of Pennsylvania, 2010.

[228] Kevin Woods, Kevin Bowyer, and W Philip Kegelmeyer Jr. Combination of multiple classifiers using local accuracy estimates. In *Computer Vision and Pattern Recognition, 1996. Proceedings CVPR'96, 1996 IEEE Computer Society Conference on*, pages 391–396. IEEE, 1996.

[229] Chih-Hung Wu. Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks. *Expert Systems with Applications*, 36(3):4321–4330, 2009.

[230] C.T. Wu, K.T. Cheng, Q. Zhu, and Y.L. Wu. Using visual features for anti-spam filtering. In *Image Processing, 2005. ICIP 2005. IEEE International Conference on*, volume 3, pages 509–512. IEEE, 2005.

[231] Y. Xie, F. Yu, K. Achan, E. Gillum, M. Goldszmidt, and T. Wobber. How dynamic are ip addresses? In *ACM SIGCOMM Computer Communication Review*, volume 37, pages 301–312. ACM, 2007.

[232] Y. Yang. Noise reduction in a statistical approach to text categorization. In *Proceedings of the 18th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval*, pages 256–263. ACM, 1995.

[233] Y. Yang and J.O. Pedersen. A comparative study on feature selection in text categorization. In *Proceedings of International Conference on Machine Learning*, pages 412–420. Morgan Kaufmann publishers, 1997.

[234] Chi-Yuan Yeh, Chih-Hung Wu, and Shing-Hwang Doong. Effective spam classification based on meta-heuristics. In *Systems, Man and Cybernetics, 2005 IEEE International Conference on*, volume 4, pages 3872–3877. IEEE, 2005.

[235] William S Yerazunis. Sparse binary polynomial hashing and the crm114 discriminator. In *2003 Cambridge Spam Conference Proceedings*, volume 1, 2003.

[236] X. Yue, A. Abraham, Z.X. Chi, Y.Y. Hao, and H. Mo. Artificial immune system inspired behavior-based anti-spam filter. *Soft Computing-A Fusion of Foundations, Methodologies and Applications*, 11(8):729–740, 2007.

[237] C. Zhang and Z. Yi. A danger theory inspired artificial immune algorithm for on-line supervised two-class classification problem. *Neurocomputing*, 73(7-9):1244–1255, 2010.

[238] Hao Zhang, Alexander C Berg, Michael Maire, and Jitendra Malik. Svm-knn: Discriminative nearest neighbor classification for visual category recognition. In *Computer Vision and Pattern Recognition, 2006 IEEE Computer Society Conference on*, volume 2, pages 2126–2136. IEEE, 2006.

[239] Junqi Zhang, Y. Tan, Lina Ni, Chen Xie, and Zheng Tang. Amt-pso: An adaptive magnification transformation based particle swarm optimizer. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E94-D(4):786–797, 2011.

[240] Junqi Zhang, Ying Tan, Lina Ni, Chen Xie, and Zheng Tang. Hybrid uniform distribution of particle swarm optimizer. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E93-A(10):1782–1791, 2010.

[241] Le Zhang, Jingbo Zhu, and Tianshun Yao. An evaluation of statistical spam filtering techniques. *ACM Transactions on Asian Language Information Processing (TALIP)*, 3(4):243–269, 2004.

[242] Pengtao Zhang and Ying Tan. Immune cooperation mechanism based learning framework. *Neurocomputing*, 148(1):158–166, 2014.

[243] Xiangrong Zhang and Licheng Jiao. Feature selection based on immune clonal selection algorithm. in chinese. *Journal of Fudan University (Natural Science)*, 43(5):926–929, 2004.

[244] Xiaolian Zhang. *Viral Immunology. In Chinese*, volume 1. Science Press, 2010.

[245] Y. Zhang and C. Hou. A clone selection algorithm with niching strategy inspiring by biological immune principles for change detection. In *Intelligent Control. 2003 IEEE International Symposium on*, pages 1000–1005. IEEE, 2003.

[246] Yuanchun Zhu, Guyue Mi, and Ying Tan. Query based hybrid learning models for adaptively adjusting locality. In *IEEE World Conference on Computational Intelligence (WCCI 2012) - IJCNN2012*, pages 429–436. IEEE, 2012.

[247] Yuanchun Zhu and Ying Tan. Extracting discriminative information from e-mail for spam detection inspired by immune system. In *Evolutionary Computation (CEC), 2010 IEEE Congress on*, pages 1–7. IEEE, 2010.

[248] Yuanchun Zhu and Ying Tan. A danger theory inspired learning model and its application to spam detection. In *Advances in Swarm Intelligence*, pages 382–389. Springer, 2011.

[249] Yuanchun Zhu and Ying Tan. A local-concentration-based feature extraction approach for spam filtering. *Information Forensics and Security, IEEE Transactions on*, 6(2):486–497, 2011.

[250] R.A. Zitar and A. Hamdan. Genetic optimized artificial immune system in spam detection: A review and a model. *Artificial Intelligence Review*, pages 1–73, 2011.

[251] Márcio Henrique Zuchini. *Aplicações de mapas auto-organizáveis em mineração de dados e recuperação de informação*. PhD thesis, Universidade São Francisco, 2003.

Index