Towards Preventing Junk Emails for Heterogeneous Network

Xiangqian Chen, Kia Makki, Kang Yen, Niki Pissinou
IT2, Florida International University, Miami, FL 33174 USA

***Abstract*—Spamming annoys most Internet users and consumes Internet resource. In the past, most research efforts were dedicated to the detection and prevention of junk emails by using content filters on the email recipient server side. Unfortunately, most studies developed have limited success on blocking the junk emails. In this paper, we propose a system framework to block spam on both the sender and the recipient sides. The proposed framework comprises several components: Email Policy Controller, Policy Email Service, Security and Exchange Information Center, and Personal Email Assistant. Compared with current prevalent content spam filter functioned passively on email recipient server side, our framework provides several tiers of reactive spam filter (not limited to content filter), and offers reactive and proactive junk email prevention to stop spam source sending them. This framework is transparent to SMTP and compatible with current email transmission system so that it's easy to be deployed. Besides functioning in high speed network, the system has some special properties in heterogeneous networks which include low speed networks such as cellular networks. Aim at most mobile devices with small LCD display and slow connection such as PDA, the Personal Email Assistant component in the system can help users read as few emails as they want without missing important information in the travel by preprocessing the emails with classification and importance analysis.**

***Index Terms*—Content filter, Junk email, Spam, SMTP**

I. INTRODUCTION

With the advent of Internet, emails have been an essential communication means for many people every day. The volume of emails has also increased exponentially day by day. One of the advantages of emails is that they allow communication among people in different parts of the world. Unlike telephone calls, emails also provide a record of message exchanged. Another advantage is that they are more efficient than other communication methods. Unfortunately, the convenience has been abused by sending large quantities of unsolicited emails to people, which is called spam or junk email.

There are several problems associated with growing volumes of junk email. One is that people spend more and more time to read and process junk emails. Another is that junk emails waste large volumes of Internet resource such as bandwidth, storage space, etc. In some cases, junk emails even bring the email servers down. Even the worst is that the stealing of confidential information such as the account number of credit card and etc.

To prevent all these, some issues including technique and law suggestion were presented. According to our literature review, most technique issues were focused on providing spam filter in the recipient side with limited success. However, some of good works intended to alleviate junk email have been published in the reference [1-8] are still valued to review.

Under Simple Mail Transfer Protocol (SMTP) email environment, it's not easy for email recipient server to prevent junk emails. Using filter to eliminate some unsolicited email before they reach users' email accounts is a conceivable method. There are some different types of spam filters discussed and compared in [1-4]. It is easy to understand that keyword-based filter is a widely used one, but it is not learning based, and the keyword pattern is set by hand with low efficiency. However, Bayesian Email Filter is learning based [1]. This type of filter is based on probabilistic theory and can be adaptive. In addition to consider raw text of email message, the Bayesian filter can increase the filter accuracy by considering domain-specific. Its performance was analyzed in [2]. It was found that despite its high spam recall rate and precision, the Naive Bayesian filter is not viable when blocked messages are deleted. With additional safety nets, however, like re-sending to private addresses, the cost of blocking a legitimate message is lower and the filter has a stable significance. Another type of essential learning method is the memory-based learning approach [3]. It attempts to classify messages by finding similar previously received messages to identify the unifying characteristics of spam messages. Both the Bayesian filter and memory-based learning filter have accurate spam filtering, outperforming clearly the keyword-based filter used in Outlook 2000, a widely used e-mail reader. Following the junk email genre evolution, the junk email detectors should also evolve to an intelligent method in order to keep the detection accuracy and the computation complex. Based on these considerations, a Spam-Detecting Artificial Immune System was proposed by using biology method [4]. It applied the artificial immune system model to protect users effectively from spam. The resulting system classifies the messages with similar accuracy to other spam

filters, but uses fewer detectors, making it an attractive solution for circumstances where processing time is at a premium. In reference [5], authors investigated the linguistic features of a corpus of junk emails, and tried to decide if they constituted a distinct genre. From the linguistic analysis, people can know junk email well and adopt more effective methods to prevent them.

In addition to filter out the junk email, some researches contributed to provide a quick normal email delivery [6]. The prioritization scheme ensures that most of the good mail is transmitted with small delays, at the expense of longer delays for junk mail. This scheme greatly improves the performance of current non-prioritized schemes.

Besides filtering out junk email, mail classification is another important email process. It helps people manage emails and save time. A self learning based email classification approach can assist users in filing messages [7]. In this research, they implemented and compared four different learning approaches: sender, keyword, TF-IDF (it is an incremental learner maintaining a table of word frequencies as message arrives) and DTree (A simple decision tree learner). In all, this work provides us with some ways to manage emails to decrease the work load of email archive, filter, etc.

In addition to adopt technique to prevent junk emails, some people suggested legal and regulatory methods. Pricing is another approach to dealing with the problem of spam. Charging a price for sending messages may help discipline senders from demanding more attention than they are willing to pay for. Price may also inform recipients about the value of a message they read it. An economic model and the results of two laboratory experiments to explore the consequences of a pricing system for electronic mail were presented in [8]. Charging postage for email causes senders to be more selective and to send fewer messages. Regardless of the exact pricing mechanism, more research is needed to identify appropriate cost functions so that they reduce the volume of communication and increase the targeting of messages without reducing communication to harmful levels.

As indicated above, most spam prevention techniques only considered to adopt filter action in recipient side. They have achieved limit success. In our proposal, we consider integrating network monitor, email sender and email recipient in one system to provide reactive and proactive spam prevention actions both in recipient side and sender side. This comprehensive and systematic solution will provide more efficient junk email prevention result. Before propose our approach, reviewing the junk email produce mechanism is useful to know our following approach.

The structure of the paper is as follows. Section II analyses current junk email produce mechanism. We introduce the junk email prevention system framework in Section III and junk email prevention analysis in Section IV. Finally we conclude and lay out some future work in Section V.

II. JUNK EMAIL PRODUCE MECHANISM

A brief overview of junk email produce mechanism is necessary to understand why spammers have had so much success and how we can block junk emails.

A. SMTP introduction

The SMTP is the accepted Internet standard for transferring emails. It belongs to application protocol in the network layer analysis. In a normal email transfer process, four computers do participate. They consist of a sender computer, an email sender server, an email recipient server, and a recipient computer. Firstly, the email is compiled and transferred from sender computer to email sender server (user email account server). Most email client software such as Outlook helps you do this. Secondly, the email sender server transfers the email to email recipient server. Finally, email client software helps recipients download the email to his/her computer from email recipient server. When affecting the transfer, the client email software is responsible for specifying the source address (‘From’ header) and domain of origin and the destination address (‘To’ header). Using the destination email address, the email sender server locates the appropriate MX (Mail Exchanger) record and determines which mail server is responsible for handling mail for that domain. When the destination mail server (or called email recipient server) is located and the mail is handed over. The SMTP protocol makes a provision for rejection (besides a delayed bounce back to sender) of the message if the destination address is invalid. If the destination is valid, the mail is delivered locally to the mailbox. The entire route that the email takes from its originating domain to its final destination is recorded in the email. After that, recipient can use email client software to check the email. Of course, email users can use web to send and receive emails.

In a special case, some email transfer process uses relay. And in such case, relay server works like email sender server does in the normal case. Relay server accepts email sending requests whether from email sender servers or sender client computers and connects email recipient servers to send emails. The main difference is that an email sender server incorporates a sender email account server in the same domain and the relay server belongs to a different domain which still supports email sending under SMTP standard.

B. Gather email address

Before sending out the junk email, spammers must do their research to find email addresses. There are several ways to gather email address. Spammers can gather the addresses from web pages, public newsgroups and web services by manual or using software to increase the efficiency. Email addresses can also be harvested from deal offer register form, organization enrollment form, etc. Depending on the region and applicable legislation, gathering email addresses without the acknowledgement of the owner of the list, from websites, or from a private list may be considered as electronic trespassing.

Some spammers gather email address by invading email database systems or by spending an acceptable price. Email active status is important information for spammers.

Spammers can detect if an email addresses is live when you respond to the received email by clicking a “remove list” link or some buttons in the email. Spammers can also exploit SMTP to validate and harvest addresses. First select a target domain with thousands of email addresses or more. Then identify this domain SMTP server. Using a mail client software and randomly selected email addresses, the software fakes the server to make it believe it is about to send an email. When asked for the destination address, the client provides the selected email address. If the address does not exist it is rejected by the email server. Otherwise, the SMTP server responds OK. The client software then breaks the connection and records the validity of the destination. This method is easy to get thousands of email addresses in short time. Though spammers can get a lot of email addresses when they invade email database system, it is not as easy to invade such administrative system. Correlatively speaking, automatic snatching email addresses software is more hazardous than other two main methods.

C. Sending out junk emails

After gathering the email addresses, the spammer can send junk emails. In normal cases, email sender server connects directly to email recipient server and uses SMTP to transfer emails. In special cases, there is a relay email server or firewall between email sender server and email recipient server. The origin email sender server does not construct the direct connection to email recipient server. The firewall or relay server connects email recipient server directly.

From the email transmitting process analysis, we can find that there are several sending bulk emails methods available. The first method is that spammers can use client software to send bulk emails by using their registered email server’s SMTP service. Most ISP’s do not support bulk mailing. They are not obliged to block spammers, although it is legal to do so. Certain Internet service providers ignore bulk mailing and provide email marketing agencies with high bandwidth lines. The second method is that spammers can locate a relay email server and send outgoing junk emails by using this relay server SMTP service. The third method is to utilize the spammers own SMTP service to send junk emails. In all, the sender can use SMTP service from public Internet Service Provider (ISP) email server, the relay server and independent server to send bulk emails. To depict easily, we use “email sender server” to designate these three email sender source computers in the following.

Cloaking or anonymity is also desired when sending junk emails. Spammers don’t want to handle any undelivered message reports or complaints from users. The SMTP protocol does not in anyway prevent the forgery of the source. In order to malign some other party, it could also be changed to reflect the victim’s address as the sender email address.

III. PROPOSED JUNK EMAIL PREVENTION FRAMEWORK

As stated earlier, the current infrastructure does not eliminate abuse. This is because SMTP considers little about email senders’ wrong activities, sending volumes of junk emails. Some people have suggested that we can modify SMTP to adapt security request. Unfortunately, SMTP is such a successful email transfer protocol that we cannot replace it although it has some weakness. Then spam filters have been recommended. These spam filters belong to application layer in nature from network analysis angle and only work passively on the recipient side. So the results are not very successful. From network structure, we can maintain the same higher layer structure and adopt some measures under this layer. In junk email prevention approach, we consider to adopt some spam prevention methods on IP layer and some measures both on recipient side and sender side. Of course, we can still adopt some current successful methods into the application layer. Because our proposed system still support SMTP and compatible with current email transmission system, it is easy to be deployed in current email transfer mechanism.

Our proposed solution provides a systematic framework to stop spam from junk email source to the end user. It consists of multiple process methods to prevent spam and protect email account from the IP layer to the application layer. This framework can record, analyze the email sender’s activities and prevent junk email. Figure 1 shows the system components of the framework. The proposed system involves Email Policy Controller (EPC), Policy Email Service (PES), Security Information Exchange Center (SIEC) and Personal Email Assistant (PEA) four main components. Each component will be defined below:

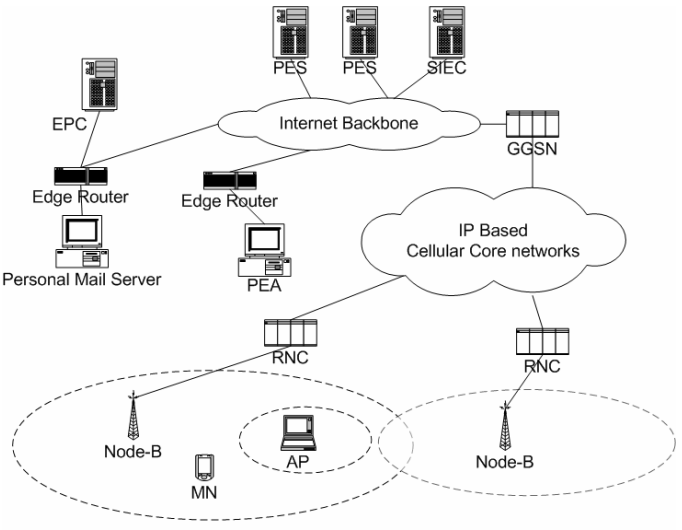

Figure 1: The proposed framework of junk email defense system

A. Email Policy Controller (EPC)

For quick process and convenience, each EPC will monitor one edge router or firewall SMTP activities. Figure 2 shows EPC structure. It includes Email Communication Monitor,

Spam Analyzer and Secure Communication Interface.

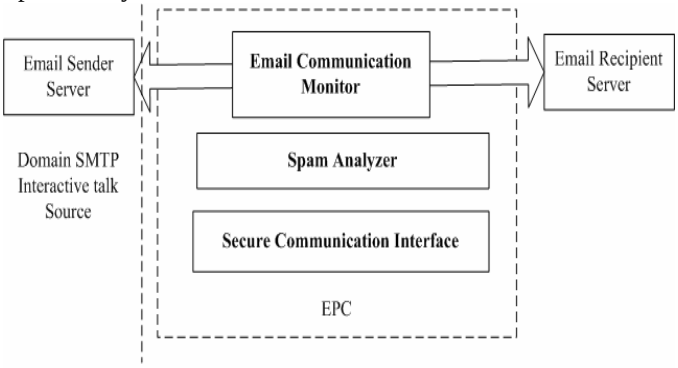

Figure 2: The structure of EPC

1) Email Communication Monitor:

Email Communication Monitor is responsible for monitoring domain SMTP activities. It examines each email communication interactive activities when the computer in this domain works as email sender server (SMTP interactive talk source). It records each email sender server address, send time, fails and/or success, etc. and the data is stored in temporary monitor database. From SMTP protocol analysis, we know the email recipient server will respond whether the destination email address is valid or not. So monitoring this type of interactive activity is feasible. Thus, each SMTP interactive activity requested from public ISP email server, the relay server and independent server in this domain will be monitored by this part. By using this part, we can monitor email source activities to prevent junk email rampancy. For efficiency consideration, if email communication monitor finds that email came from a registered white list computer such as PES, it will omit monitor activity.

2) Spam Analyzer

Spam analyzer periodically analyzes every monitored email transmission status by accessing the monitor data. If the email transmission successful rate is lower than a threshold, analyzer considers this sender as junk email source. Then analyzer records this junk email source address information in email block list database. Usually the block list records the spammers' IP address and DNS (Domain Name System) name. For high protection request, the block list even includes MAC (Media Access Control) address by contacting the DHCP (Dynamic Host Configuration Protocol) server of the sender. Under this condition, if the system record the spammer activity, it is not easy for spammer to evade the trace and block action because every network card has a unit MAC address. Though the computer can change IP address (under DHCP protocol), the MAC address is unique.

3) Secure Communication Interface

Secure Communication Interface is responsible for EPC communication with other parts in the system. EPC periodically reports its new block list to SIEC and uses this part to get updated information of the block list and the white list from SIEC. All of data exchanges are under security environment such as data encryption, authentication and etc. SIEC can inform EPC updating its EPC block list and white list based on periodical or other schedule mechanism.

B. Policy Email Service (PES)

Based on standard SMTP, PES enhances some functions and makes email communication resilient and secure. From this point, PES is an email server with enhanced junk email prevention function. Figure 3 shows PES structure. It includes several main parts: Incoming Spam Protector, Spam Feedback Evaluation Part, Special Email Utility Part, Spam Sender Protector and Secure Communication Interface.

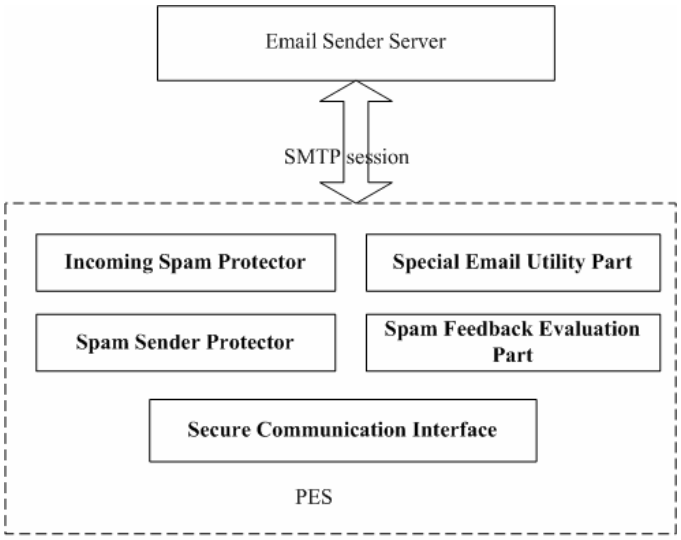

Figure 3: The structure of PES

1) Incoming Spam Protector

Incoming spam protector is responsible for processing SMTP email transfer request when an email sender server constructs a SMTP connection to this PES. Besides processing SMTP request, Incoming Spam Protector also provides several layers of email protection that prevents incoming junk email.

In a SMTP interactive session, when an email sender server tries to contact PES, incoming spam protector starts to work. The first spam prevention layer is that the protector checks the DNS address provided by the email sender server (sender provides its DNS by SMTP command "Hello"). If the protector finds that sender provides fake DNS, it will reject the sender email sending request. Secondly, the protector compares the email sender server (email sender server is a computer that has SMTP interactive sessions with an email recipient server) address with email server block list. If the email sender server address is in the block list, the protector will reject the sender email sending request. Thirdly, the protector checks sender (email user) email address provided by email sender server (email sender server provides sender email address by SMTP command "MAIL FROM"). If the sender's email address or sender server address is in the recipient email account block list,

the protector will reject the sender email sending request. Fourthly, spam protector analyzes the incoming message header to check whether this email is a spam. PES receives the message from sender by SMTP "DATA" command if the communication passes the above three layers protection. Then incoming spam protector analyzes message header ("received: from") lines to see whether they include fake email transfer routing information or block address. For example, if it finds the routing path included any unnecessary computer, it will consider this email as spam. Under email message header analysis, it can find email disguise activities. Besides message header's spam prevention, Incoming Spam Protector also provides spam content filter. It can adopt current prevalent content filter algorithm such as keyword filter or Bayesian Email filter to filter the junk email. This is considered as fifth layer spam protection.

From first layer to third layer, the protector provides accurate spam analysis result during SMTP "interactive talk" between email sender server and the protector. And if the protector finds the incoming email is a spam, it will stop the SMTP interactive session immediately and record this information. If the protector finds the incoming email is a spam in the fourth layer protection, it will not transfer the email content to the recipient email user account and delete this email. If the content filter spam prevention layer considers the incoming email as spam, this email will be deleted automatically or transferred to recipient email user account spam folder based on recipient user previous subscription because content filter cannot guarantee the spam estimation accuracy is 100%.

To improve performance, Incoming Spam Protector may omit fourth layer and fifth layer inspection when the incoming email is from a white list server. Of course, it still considers a personal email account block list settings. Incoming spam protector also considers incoming email is not spam when its source is in the destination email account white list to save processing time.

In our approach, we try use many types of block lists and white lists to improve system spam protection accuracy and performance. Though all the above spam prevention failed and junk email entered user account in some time, we can use recipient user's feedbacks to increase it future estimation accuracy.

2) Spam Feedback Evaluation Part

Spam Feedback Evaluation Part is responsible for evaluating senders sending activities under recipient user's help. If the email is not in any types of white lists and block lists, spam evaluation part will record this email related information such as sender user email address, send server address and etc. It will also record the recipient's activities. For example, if the recipient moves the email to the spam folder of his/her account storage space, this email sender's server address and email address will be added in recipient's block list and Spam Feedback Evaluation Part will consider this email as spam and record it. This Part periodically analyzes system recorded information. If it finds that the spam rate sent from one sender's server is higher than a threshold, it will consider this sender server as a spam source and add it to its block list. After that this email server will reject this source's email sending activities in the future. Under considering email recipients' responses, PES and the system provide higher spam protection accuracy than current prevalent normal content filter.

Besides providing spam Feedback evaluation, system also records relay servers' spam transmission cases and report to SIEC through Secure Communication Interface.

3) Special Email Utility Part

Special Email Utility Part is responsible for special email use such as searching people, religion, politics and etc. This part defines special email use format, analyzes this type of email and provides analysis result to administrators to let them decide whether broadcast this special use email.

In current environment, if you want to use email as tool to search relatives, friends, and etc, you have to send millions of emails like spammer does. This method wastes users' time and Internet resource. Under PES Special Email Utility Part help and administrator's control, people can broadcast special use email easily without sending volumes of emails.

Under PES, it defines special email format for searching people including published searching email address and content format. For analysis easier, the searching people email subject and content are defined by standard XML format. If you wish to find a friend, you only need to send emails with standard format to the special email addresses for searching people (suggestion: this email address name is preferred to be the same in every domain) in all the domains you want to search. Special Email Utility Part then analyses this email and transfer its analysis result to email server administrators. Special Email Utility can also control the number of this type of email from a specific IP, email address or etc by using a counter. Of course, PES can let the same IP send many searching people emails. Based on Special Email Utility's analysis results, administrators can decide whether broadcast this email to the special user groups or all users in this domain or reject this searching request. When this request transfers to recipients' account, Personal Email Assistant will read this searching people email and give recipients notices. In the whole process, all people involved in this process don't know each other emails. When the domain user considers that the sender is his/her friend, he/she can answer Personal Email Assistant with YES and provide other information. Then Special Email Utility Part automatically informs him/her the source sender email address.

The whole progress is controlled under security environment. PES stores and verifies the email source IP. Other types of email communications utilities use the same progress. Of course, not all the type of special use emails is transferred to all the users in the domain. Some types of email use broadcast are under the users' subscriptions.

In some distinctive application cases, PES has an accounting part to calculate some special types of emails from designate

source. This is for marketing and charging purpose.

4) Spam Sender Protector

Spam Sender Protector authenticates each email transmission activity when PES works as a SMTP sender server or email relay server (in some networks have firewalls). It authenticates the user information such as email address registered in this mail server, sender IP address under relay transmission environment or etc. All these actions are to make sure that the email sending activities are under authentication control. Besides providing authentication, Spam Sender Protector also prevents spam by each user email destination block list. If the users want to send emails in their destination block lists, PES will reject their requests.

Spam Sender Protector stores and manages each user email destination block list. Users cannot send email to their own block destination lists or modify them. These lists are managed by Spam Sender Protector and are obtained from other PES user block source list. For example: suppose user Alfred in PES "A" blocks user Tom in PES "B". PES "A" will report this to SIEC and SIEC will inform this to PES "B". Then user Alfred address will be added in user Tom's destination block list. And user Tom cannot send email to user Alfred any more in the future. If Alfred blocks all users in PES "B", then all users in PES "B" cannot send email to Alfred in the future unless Alfred changes his mind.

5) Secure Communication Interface

Secure Communication Interface is responsible for PES communication with other parts in the framework. PES periodically reports its new produced block list including server block list and personal block list to SIEC and get new updated block lists information and white list from SIEC periodically. All of data exchanges are under security environment.

C. Security Information Exchange Center (SIEC)

Security Information Exchange Center, a distributed database, is a higher controlled mechanism in the whole framework. Figure 4 shows SIEC structure. It includes Register Management System, Information Exchange System, Global Spam Evaluation System and Secure Communication Interface.

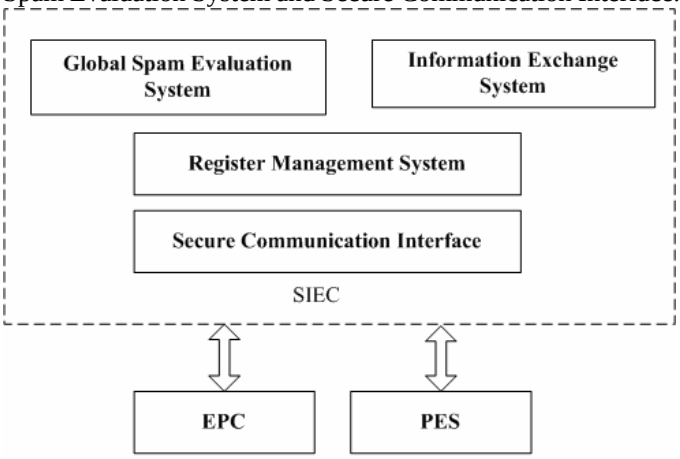

Figure 4: The structure of SIEC

1) Register Management System

Register Management System is responsible to manage EPC, PES, white lists and block lists register. Administrators can modify the block lists.

2) Information Exchange System

Information Exchange System is responsible for exchange information between EPC and SIEC or PES and SIEC. All the information exchange is under security control.

3) Global Spam Evaluation System

Global spam evaluation system analyzes every EPC and PES reported local spam source information and decides whether the local spam computer is a global spam source. If Global spam evaluation system considers a source as a global spam source, it will inform this to every EPC and PES.

4) Secure Communication Interface

Secure Communication Interface is responsible for SIEC communication with PES or EPC. In some cases, SIEC reports spam source to ISP intelligent edge routers or ISP administrators.

D. Personal Email Assistant (PEA)

Personal Email Assistant is an intelligent part. It can be run in user's own computer or as one part of email service in email server. It works between PES and email client reader. PEA helps user spend little reading time without missing important message. And at the same time, it provides email management. Figure 5 shows PEA structure. It includes Email Classification Analyzer, Email Importance Analyzer, Email Subscription Management Part, Spam Management Part and Secure Communication Interface.

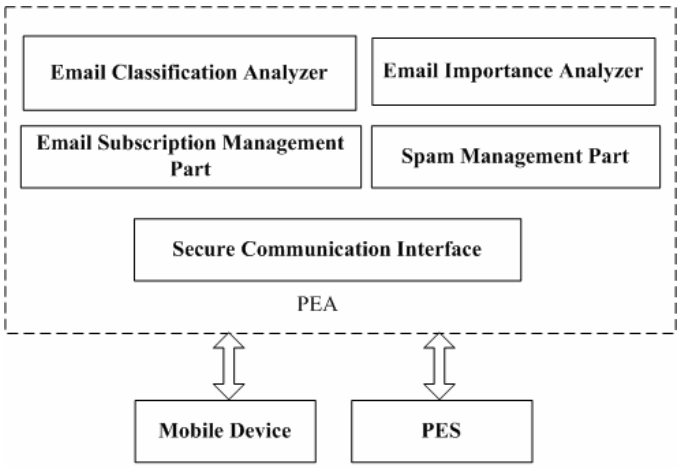

Figure 5: The structure of PEA

1) Email Classification Analyzer

Email Classification Analyzer helps users classify emails according to email communication purpose such as business, friend, religion, etc., based on user configuration.

2) Email Importance Analyzer

This component analyzes email importance based on user's

address book, white list, user's important list, and other configurations. It ranks the important list, white list, and content analysis as different weight to calculate the important values of the emails and sort the emails according to those values. When user uses mobile device such as PDA to connect email server to get emails, PEA transfers emails to the mobile device according to important weight values and user previous threshold configuration.

The email classification and important analysis are very important especially when users can only use small reading screens and low speed connection mobile devices such as PDA to read emails in travel time. In such condition, users want to read few emails. At the same time, they don't want to miss important information such as stock information, limit time offers, important businesses, and etc.

3) Email Subscription Management Part

Email Subscription Management Part is responsible to manage the email subscription lists from its PES and other email sources. When users don't want to receive some email subscriptions, they only need move their received emails to un subscribed folder and Email Subscription Management Part will help them complete unsubscribe.

4) Spam Management Part

Spam Management Part is responsible to report junk emails to PES and PES will renew their spam evaluation system and improve its accuracy. When users consider some emails (after PES spam filter) as junk emails, they only move these emails to junk email folder and Spam Management Part will do the following including adding these emails to the block list, reporting them to PES and etc. Of course, if users made mistakes to report the normal emails as spam, they only need to move the emails from junk email folder back to normal received email folder and Spam Management Part will do the rest.

Spam Management Part can also protect users' email addresses. Destination user account active status is an important marketing factor to spammers. Through prohibiting source program code embedded in the email content running, Spam Management Part prevents email source from knowing whether the destination recipient account is still active. Of course, the recipient can let these codes to run to get the whole email content when he/she considers it as a normal email.

5) Secure Communication Interface

Secure Communication Interface provides secure communication environment between PEA and PES or PEA and mobile devices.

IV. JUNK EMAIL PREVENTION SYSTEM ANALYSIS

A. Protect email address

Our proposed system can prevent spammers from gathering email address with automatic snatching email software. This is done by EPC monitor and PES authentication. In our system, when the spam software tries the recipient email server, the sending email successful rate is very low so that EPC can easily detect this spam source and inform edge router. And PES will also stop email service for this spammer's SMTP sending request in a short time. In our proposed system, spammer has difficulty to snatching email addresses in the domain. Besides EPC and PES protection, PEA also provides email account active status protection by prohibiting source program code embedded in the email content running.

Prevent user from receiving junk email

If spammer sends junk emails by registered email server, normally these transmission emails will pass the client computer, email sending server computer, email receiving server computer, and recipient client computer. Supposed email sender server and email recipient server are both installed with PES. Under this case, there are several layers installed in sender side and recipient side for email protection. Firstly, PES Spam Sender Protector prevents sender from sending some types of junk emails. Secondly, recipient PES Incoming Spam Protector prevents email users from receiving junk emails. If junk emails pass above two protections, PEA can help PES increase spam filter accuracy and the recipient user will not receive spam from this spam source in the future. And email sender server PES will block this spam source account sending email activity in a short time.

When spammer sends junk emails by email relay server, the email protection methods are very similar to the above case if email relay server and email recipient server are both installed PES. The only difference is that PES Spam Sender Protector will authenticate relaying request computer's information such as IP address and etc not the email account information of the sender in the previous case.

When spammer sends junk emails with independent email server, our proposed scheme still have some methods to prevent them from sending junk emails. First, EPC will monitor the spam source activities and report it to SIEC. Then SIEC will notify PES shortly. And recipient PES and PEA still work to prevent junk emails.

In our proposed scheme, EPC, PES can work corporately or independently under SIEC control. Even though junk emails pass the layer upon layer spam preventions, PES can still block this spam source in limited time because the system adopts recipients' responses information.

From above analyses, it shows that it is difficult for spammers to send a large amount of junk emails through our system.

B. Provides easy way for special email communication use

Compared to current junk email filter, our system provides an easy way for special email uses. For example, currently, if you want to search a person by using email, you need try millions of email address. This method has low efficient, waste Internet resource and hassle millions of people.

In existing email system mechanism, we face a dilemma to search people by email without hassling millions of people. In our proposed system, PES Special Email Utility Part can ease

this problem by a defined email format and standard process.

V. Conclusions and Future Work

In this paper, we have introduced and discussed junk email produce mechanism and proposed our junk email prevention system. Compared to current spam filter passive response to spam, our proposed system provides both proactive and reactive junk email preventions with the consideration of recipients' feedbacks information. And the proposed system provides email protection covered from application layer to IP layer, sender side and recipient side. And some prevalent spam filter can still be incorporated in PES. We specially analyze the different components of the model and their interactions, which provide a novel approach to enhance the spam prevention.

Future work will include design of various parts under the proposed framework. Hence, some important parameters to help system run more effectively and some analytical models for the proposed architecture can also be developed.

References

[1] Sahami, M., Dumais, S., Heckerman, D., and Horvitz, E., "A bayesian approach to filtering junk e-mail," *AAAI-98 Workshop on Learning for Text Categorization*, 1998.

[2] Androutsopoulos, I., Koutsias, J., Konstantinos, V., Chandrinos, V., Paliouras, G., and Spyropoulos, C. "An evaluation of Naive Bayesian anti-spam filtering", *Proceedings of the workshop on Machine Learning in the New Information Age*, 11th European Conference on Machine Learning, Barcelona, Spain, pp. 9-17, 2000.

[3] Androutsopoulos, I., Koutsias, J., Paliouras, G., Karkaletsis, V., Sakkis, G., Spyropoulos, C., & Stamatopoulos, P., "Learning to filter spam e-mail: A comparison of a naive bayesian and a memory-based approach", Workshop on Machine Learning and Textual Information Access, at 4th European Conference on Principles and Practice of Knowledge Discovery in Databases (PKDD), 2000.

[4] Terri Oda, Tony White, "Increasing the Accuracy of a Spam-Detecting Artificial Immune System", *Evolutionary Computation*, CEC'03, 2003.

[5] Constantin Orasan, Ramesh Krishnamurthy, "A corpus-based investigation of junk emails", *Proceedings of LREC-2002*, Las Palmas, Spain, 2002.

[6] Richard Daniel, Williamson, "Email Prioritization: reducing delays on legitimate mail caused by junk mail", *Proceedings of USENIX 2004 Annual Technical Conference*, pp. 45-58, 2004.

[7] Elisabeth Crawford, Judy Kay, "Automatic Induction of Rules for e-mail Classification", ADCS2001, *Proceedings of the Sixth Australasian Document Computing Symposium*, pp 13--20, Coffs Harbour, NSW Australia, 2001.

[8] Shyam Sunder, Rahul Telang, James Morris, "Pricing Electronic Mail To Solve the Problem of Spam," Available: http://www.econ.upf.es/docs/seminars/ sunder.pdf