스팸 메일 차단 신뢰도 향상을 위한 SMBC 플랫폼 설계

종신회원 박 노 경*, 정회원 한 성 호*, 서 상 진*, 진 현 준*

A Design of the SMBC for Improving Reliability of Blocking Spam Mail

Nho-Kyung Park* ***Lifelong Member***, Sung-Ho Han*,
Sang-Jin Seo*, Hyun-Joon Jin* ***Reguler Member***

요 약

현재 인터넷 상에서 신속한 의사소통을 위해 사용되는 전자우편의 증가는 상업적 의도를 가진 상품 홍보 수단으로 악용되며, 많은 사회적 문제를 유발시키고 있다. 이에 다양한 스팸 차단 필터 기술이 개발되고 있으나, 차단 필터의 성능에 따라 정상 메일을 스팸 메일로 오인하여 사용자의 시스템 이용 신뢰도를 크게 저하시키고 있다. 본 논문에서는 스팸 메일 차단 시스템의 이용 신뢰도를 높이기 위해 Privacy 기반의 스팸 메일 복구 기법이 적용된 SMBC(Spam Mail Blocking Center) 스팸 메일 차단 플랫폼을 설계 및 제안한다. SMBC는 Proxy Server 기반의 스팸 차단 시스템 프레임 레이어로 설계되며, 물리적으로 임의의 위상(Topology)로 구축 가능하여, 플랫폼 구현시 유연한 모듈/구성 레이어 개발이 가능하다. 제안된 SMBC 플랫폼은 기존 스팸 메일 차단 시스템에 비해 처리 부하와 차단 필터의 오인률을 최소화하여 시스템 이용 신뢰도를 높일 수 있도록 설계되었다.

Key Words : Spam Mail Blocking, SMBC Platform, False-Positive mail recovery, Privacy Information

ABSTRACT

While the E-mail is a important way of fast communication in these days. it is real that the E-mail is often misused as a commercial advertisement method and creates many social problems. Even though various filtering techniques for blocking spam mails have been developed, reliability of mail systems is decreased by misreading normal mails as spam mails, i.e. false-positive errors. In this paper, the SMBC(Spam Mail Blocking Center) platform employing spam mail recovery method based on privacy information is proposed and designed. The SMBC is designed in frame layer based on spam blocking system of proxy server and can be physically implemented in various topology so that flexible development with layered module is possible. Using privacy information makes the proposed SMBC platform minimize processing load and false-positive error rates so that it can improve mail system reliabilities.

Ⅰ. 서 론

전자우편(E-Mail)은 인터넷 이용자 중 84.6%가 보유하고 있으며, 정보통신 사회의 중요한 의사소통 수단이 되고 있다. 그러나 전자우편의 사용 증가는 상업적인 의도로 제작된 스팸 메일 광고 시장을 활성화시키고, 특히 음란 스팸 메일과 같은 불법 메일이 성인뿐만 아니라 아동 및 청소년에게도 무차별적으로 전송되어 건전한 사회 풍토에 저해 요인이 되고 있다[7].

* 호서대학교 정보통신공학과 (nkpark@office.hoseo.ac.kr)
논문번호 : KICS2005-07-310, 접수일자 : 2005년 7월 28일
※ 본 과제(결과물)는 교육인적자원부와 산업자원부의 출연금 및 보조금으로 수행한 산학협력중심대학 육성사업의 연구결과입니다.

현재 스팸 메일 차단 시스템은 스팸 정보 기반의 키워드 검색 및 빈도수, 매칭 규칙에 따라 스팸 메일을 추출한다. 그러나 다양한 신규 스팸 유형에 대해 다수의 차단 필터를 교차 검사하는 과정에서 차단 시스템의 성능에 따라 달라지지만 정상 메일이 스팸 메일로 오인(False-Positive Error)되는 빈도수는 여전히 높다. 특히, 메일 수신의 중요도에 따라 이용자에게 치명적인 오류를 범할 수 있으므로, 스팸 메일 차단 기술 및 시스템을 구축하는데 스팸 메일 판정 오인률을 최소화시키는 문제는 매우 중요하다.

본 논문에서는 오인된 정상 메일의 발생률을 줄이기 위해 Privacy[3] 기반의 복구 기법을 적용한 SMBC 플랫폼을 설계한다. SMBC 플랫폼은 기존의 스팸 메일 필터를 이용하여 스팸 차단 작업을 수행하여 정상 메일과 스팸 메일을 분류한다. Privacy 기반의 오인된 정상 메일 복구 기법은 스팸 메일을 보관하는 독립된 시스템에 적용되어 필터 차단률과 판정 오인률 최소화를 통해 시스템의 신뢰도를 향상시킨다.

논문의 구성은 2장에서 기존의 스팸 메일 차단 시스템 의 유형 및 대응 기술에 대한 관련 연구를 살펴보고, 3장에서는 Privacy 정보 기반의 오인된 정상 메일 메일 복구 기술을 설명한다. 4장에서는 복구 기법을 적용한 SMBC 플랫폼의 설계에 대해 설명하고, 5장에서 결론 및 향후 연구과제에 대해 기술한다.

Ⅱ. 관련 연구

2.1 스팸 메일 차단 시스템 유형

스팸 메일 차단 시스템은 적용 분야와 구현 기술을 기준으로 구분된다. 적용 분야에 따른 차단 시스템 유형은 네트워크 트래픽을 원천 차단하는 서버형과 단말기에서 차단하는 클라이언트형으로 구분된다[7].

서버형 스팸 차단 시스템은 스팸 메일 차단을 위해 가장 많이 사용되는 차단 시스템 유형이다. 서버 기반의 게이트웨이(Gateway)형 서버는 메일 서버가 위치해 있는 내부 네트워크와 외부 네트워크가 분리된다.

클라이언트형 스팸 차단 시스템은 사용자의 PC에 설치되어 메일 서버에 일정 시간마다 접근하여 메일 박스로부터 수신된 스팸 메일을 삭제하는 기술이다. 구현 기술에 따라 프록시(Proxy) 서버형과 에이전트(Agent)형으로 구분된다.

프록시 서버형은 일정 시간 간격으로 스팸 필터링하며, 사용자는 일정시간마다 필터링된 메일을 수신받는다. 이러한 기술은 사용자에 대한 스팸 도달 가능성을 최소화시키지만, 많은 시스템 자원을 필요로하며, 웹에서 사용할 수 없는 문제점을 가진다.

에이전트형 스팸 메일 차단 시스템은 PC에 설치되어 메일 클라이언트에 부가적인 접근이 불필요한 시스템이다. 에이전트 기술은 스팸 메일을 확인하는 시간 간격이 존재하므로, 해당 시간 간격 이내에 스팸 메일이 유입된 직후 사용자가 메일을 확인되는 결함이 있다. 그러나 전체적으로 웹 메일을 필터링 할 수 있는 장점이 있다.

2.2 스팸 메일 차단 필터링 기술

스팸 발송 기술과 안티 스팸 기술은 발생-대응 관계를 반복하며 상호 대응된다. 이와 같은 대응관계를 고려한 스팸 메일 차단 기술 적용을 위해 SMTP와 EML을 하나 또는 전체를 검사 처리하여 스팸을 차단한다. 스팸 메일의 발송 유형은 크게 7가지 정도로 구분할 수 있다[7].

Serialization 발송 유형은 스팸 메일에 주어진 문자열 사이에 유일한 값들을 첨부하는 발송 기법이다. 첨부 방법 종류는 임의의 수를 첨부하는 random incremental, 단위 시간 간격마다 일정한 값을 첨부하는 Time Stamped, 특정 키워드를 첨부하는 Keyword Inserting, 사전 순서식으로 값을 첨부하는 Dictionary Serialization 등이 있다. 이러한 Serialization 발송 유형은 스팸 메일을 해쉬 정보를 저장하여 스팸 메일 차단을 수행하는 체크썸 기술이 무효하므로, 정규식과 필터링 스크립트 등을 이용하여 수신된 스팸 메일을 구별할 수 있는 정교한 필터링 스크립트를 적용해야 한다.

HTML Cloaking 발송 유형은 HTML 트릭을 이용하는 방법으로 본문의 HTML 코드 안에 빈칸 혹은 유니코드 등을 삽입하는 방법이다. HTML stuffing, Space Stuffing 등이 이러한 HTML Cloaking의 대표적인 발송 유형이다. 이러한 HTML Cloaking 발송 유형에 대처하기 위해서는 HTML Purification을 통해 빈칸/유니코드를 삭제하여 발송자의 메일 원문을 추출하여 스팸 패턴 필터링 기술을 적용해야 한다.

Graphical 발송 유형은 부가 정보없이 스팸 내용을 이미지로 작성하여 전송하는 스팸 메일 발송 유형이다. 이러한 스팸 내용이 특정 이미지 포맷으로 구성되어 있는 경우 우선, 이미지 패턴 작업을 수행

하여 이미지 내에 URL, 단어, 번호 등의 내용을 추출한다. 추출된 내용을 조합하여 필터링 스크립트를 적용하여 스팸 메일을 차단한다.

Other Encoding 발송 유형은 기존의 메일 포맷이 아닌 비 표준 메일 포맷으로 인코딩하여 발송하는 스팸 메일 전송 유형이다. Base64, QP, 유니코드 등으로 인코딩되기도 하며, 이러한 발송 유형에 대한 스팸 차단 기술 적용은 수신 메일의 인코딩 타입을 분석 및 추출하여 디코딩하여 처리하거나, 자체 디코더를 통해 메일을 디코딩한 후 스팸 메일 차단 기술을 적용한다.

Foreign 발송 유형은 영어, 중국어, 일본어 등의 외국어로 표시되는 메일이며, 이러한 발송유형은 휴리스틱 기법과 해외 데이터베이스를 활용한다.

Personalized 발송 유형은 특수 개인이 자신만의 고유한 포맷으로 스팸 정보를 생성하여 발송하는 유형을 의미한다. 이러한 개별적인 고유 스팸 유형을 차단하기 위해서는 스팸 메일 내에 본문의 패턴 분석을 수행하여 스팸 메일을 차단한다.

Syntax Noise 발송 유형은 메일 내용 중 무의미한 기호나 문자를 이용하여 스팸 메일을 발송하는 유형을 의미한다. 문자로 구성된 스팸 연상 발송 유형은 다른 문자열 기반의 스팸 메일 차단 기술과 유사하게 정규식이나 특수 문자, 혹은 무의미한 기호 등을 삭제하여 스팸 유형화 직전의 원문으로 복원하여 스팸 메일 차단을 위한 정규식을 적용한다.

이와 같이 스팸 메일의 발송 유형 다양한 형태로 스팸 정보 전달을 위한 포맷이 동적으로 생성된다. 그러므로 스팸 메일 차단 기술은 최소 시간에 동적인 발송 유형과 정적인 관례적 처리 특성을 고려하여 적절한 차단 기술의 적용이 효과적으로 이루어져야 된다.

Ⅲ. Privacy 기반의 신뢰도 향상 기술

3.1 개요

스팸 메일 차단의 신뢰도를 향상시키기 위하여 Privacy기반의 정보를 이용한 False-positive 메일 복구 기술을 제안한다.

기존의 스팸 메일 차단 방식은 스팸 정보 영역에 특정 정보를 계층적 데이터 풀로 구성하여 스팸 메일을 차단한다. 그러나 이러한 접근 방식은 필터 패턴 생성보다 더 많은 정보 생성을 고려해야 되는 문제점을 가지고 있다. 이와 같이 접근 방식에서 기인된 문제점의 근본적인 해결책 제공을 위해 Privacy 정보[3] 기반의 False-Positive 메일 판정 방식을 이용한다. 특히, 기존의 교차 필터링 처리시 발생된 False-Positive 메일을 복구하여 스팸 메일 차단 신뢰도를 향상 시킬 수 있다.

Privacy 메일 판정을 위한 학습 시스템은 수신되는 Privacy 메일의 내용을 분석하여 특정 Privacy 영역에 포함된 keyword들에 대한 가중치를 다르게 부여하여 판정시 참조한다. 그리고 추출된 Privacy 정보를 Privacy 수집 DB에 누적시켜 Privacy 정보 참조 구조를 확장한다. Privacy 기반의 메일 복구 처리시 수집된 Privacy 정보는 베이시안[1,2] 조합을 이용하여 영역에 따라 분류 저장한다.

3.2 False-Positive 메일 복구 처리 과정

False-Positive 메일 복구 과정은 크게 문장을 구문 분석하고, Privacy 속성을 추출한 후, Privacy 속성의 가중치를 더해서 False-Positive 메일을 판정하는 과정으로 구분된다. 이와 같은 처리를 위해 복구 과정은 한국어 구문 분석기, 토큰 생성기, Privacy 속성 추론 기관, 판정 모듈로 구성된다. 한국어 구문 분석기는 구문 분석된 키워드와 구문의 품사 등의 정보가 제공된다. 토큰 생성기는 분석된 구문을 속성(Property) 형태로 저장한다. Privacy 속성 추론 기관은 분석된 구문 키워드들을 Privacy DB를 참조하여 Privacy 속성 및 Privacy 속성 후보자 여부를 추론한다. 판정 모듈은 추론 모듈로부터 추출된 Privacy 속성 및 Privacy 속성 후보자 키워드와 가중치를 조합하여 False-Positive 메일을 판정한다. 그림 1은 전체적인 복구 과정을 도시하고 있다.

본 논문에서는 False-Positive 메일 복구 처리를 위해 메일 구성 내용을 5개의 튜플로 정의한다. 여기서, Pk는 Ck에게 종속되는 Subset 임을 알 수 있다. 그림 2는 메일 구성 튜플의 정의를 나타내었다. 그림 3은 정의된 튜플들을 이용하여 Privacy 기반의 False-Positive 메일 복구 알고리즘을 나타내고 있다.

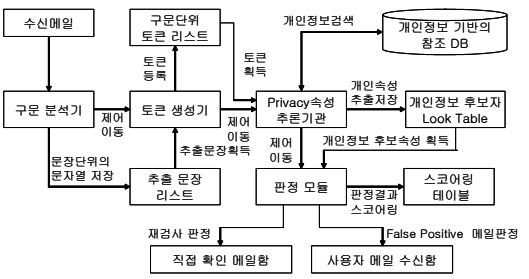

그림 1. Privacy 정보 기반의 False-Positive 메일 복구 전체 처리 구성도

본 논문에서는 베이시안 기반의 필터링 수행시 가능한 확률적인 오판을 최소화하고 이분법적인 분류를 배제하기 위해 직접 확인을 위한 False-Positive 후보자 메일 보관함(confirm mailbox)을 추가 적용하였다.

N, S, FP, FN ∈{S, P, C, V, E}
* 단, M = {N, S, FP, FN}
· M : {N, S, FP, FN}인 튜플들의 집합
· N : 정상 메일
· S : 스팸 메일
· FP : False-Positive 메일
· FN : False-Negative 메일
· S_k : {S_1, S_2, ... S_i}인 스팸 키워드들의 집합
· P_k : {P_1, P_2, ... P_i}인 Privacy 키워드들의 집합
· C_k : {C_1, C_2, ... C_i}인 Privacy 후보자 키워드들의 집합
· V_k : {V_1, V_2, ... V_i}인 P_k, C_k 추출 동사 키워드의 집합
· E_k : S, P, C, V 튜플에 속하지 않는 키워드

그림 2. 복구 기술 적용을 위한 메일 구성 튜플 정의

```
-Input: Tuple FP
-Output: A judgement on a FALSE-Positive mail
[1] Initialized the prototype and copy a new e-mail.
[2] Analysis Body of Mail using KLT-Parser.
[3] Make Data-Structure for the protype.
[4] while(until reach end of a statement-list) {
[5]    read a statement from a statement-list.
[6]    Make a token-list for retrieving    privacy-
       properties
       }
[7] while(until reach end of a token-list) {
[8]    read a pair of tokens from a token-list
[9]   retrieve properties of Ck in the privacy DB
      for privacy-information
[10]   if(a retrieved property is a pair of tokens
       for a candidate)
[11]   insert properties of Ck of candidate into a
       lookup table.
       }
[12] while(until reach end of a lookup table) {
[13]    read a property of Ck from a lookup table.
[14]    validate relation of Pk on a Ck.
[15]    if(Is a validated property) scoring a field
         related of privacy
       }
[16] processing analysis of a scoring table.
[17] judge a inputed e-mail FALSE-positive
[18] if(a result of judgment is a FALSE-positive mail)
[19]      move a mail to user mailbox
[20] else if(a result of judgment is not a FALSE-pos-
      itive mail)
[21]      leave a mail in spam mailbox.
[22] else
[23]      move a mail to unsure-folder.
[24] free resources allocated the RF-engine.
```

그림 3. 개인 정보 기반의 False-Positive 메일 복구 알고리즘

Ⅳ. SMBC 플랫폼 설계

4.1 SMBC 플랫폼 개요

SMBC(Spam Mail Blocking Center)는 Proxy Server 기반의 스팸 차단 시스템 프레임 레이어로 설계된다. Proxy Server 기반의 차단 프레임은 물리적으로 임의의 위상(Topology)로 구축 가능하여, 플랫폼 구현시 유연한 모듈/구성 레이어 개발이 가능하다. 그림 4는 SMBC 플랫폼의 전체 구성도를 나타내고 있다.

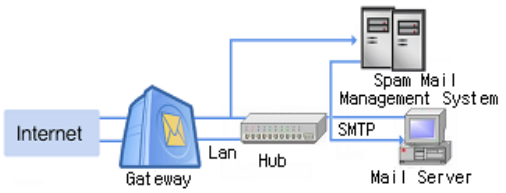

그림 4. SMBC 플랫폼의 전체 구성도

SMBC는 터널형 스팸 메일 차단 프레임에 비해 필요시 스팸 메일로 분류된 메일이 복구가 가능하다. 그리고 스팸 차단 프레임과 메일 트래픽의 상호 독립되어 네트워크 스트림 채널을 분산시켜 병목현상을 최소화시킬 수 있다.

4.2 기본적인 SMBC 플랫폼 구조 및 처리

본 논문에서 설계되는 SMBC 플랫폼은 크게 스팸 메일 차단 서버와 H/W 기반의 FA(Filtering Accelerator)를 포함한 스팸 메일 보관 시스템으로 구분된다. 각 구성 모듈은 S/W와 H/W로 구성되며, 상호 비동기적 연동 체계를 통해 작업을 분산처리한다. 그림 5는 SMBC 플랫폼의 처리 구성도를 나타내고 있다.

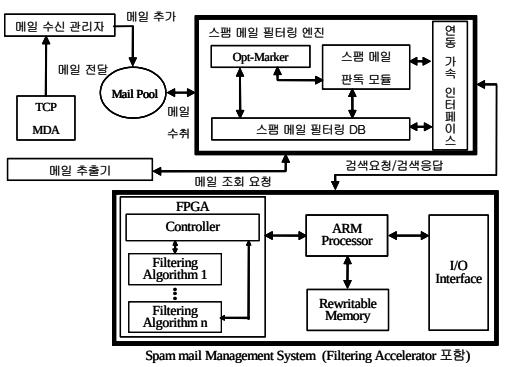

그림 5. SMBC 플랫폼 처리 구성도

메일 차단 서버는 TCP/IP 프로토콜을 통해 메일 전송 관리자(MDA)가 메일 수신 관리자에게 메일을 전달한다. 메일 수신 관리자는 전달된 메일을 메일 보관함(Mail Pool)에 보관한다. 스팸 메일 차단기는 수신된 스팸 메일을 검사하고 처리 결과에 따라 스팸 메일 보관함이나 메일 보관함으로 메일을 이동 보관 처리한다. 처리 결과는 스팸메일 필터링 DB에 보관하여 지식 정보를 훈련(Training)시킨다. 신속한 스팸 메일 처리 및 복구를 위해 스팸 메일 차단 장치는 임베디드 환경에서 구현되며, 포맷 해석 및 판정 처리를 위해 FA 가속기와 연동된다.

4.3 SMBC의 False-Positive 메일 복구

SMBC 플랫폼 내에 스팸 메일 관리 장치의 복구 엔진 처리 과정은 기존의 Proxy Server형 스팸 메일 차단 시스템과 유사한 처리 흐름을 가진다. 그러나, 스팸 메일로 판정되면 스팸 메일 보관함으로 메일을 이동하게 되며, 스팸 메일 보관함의 False-Positive 메일 복구 엔진이 단위 시간 주기로 스팸 메일 보관함에서 False-Positive 메일을 검색, 판정, 복구 작업을 수행한다. 그림 6은 False-Positive 메일 복구 처리 과정을 간략히 나타내고 있다.

SMBC 스팸 메일 차단 서버는 스팸 정보 기반의 필터링이 우선 적용된 후, False-Positive 메일 복구 시 Privacy 정보 기반의 필터링이 적용된다. 그러므로 스팸 메일 차단 서버의 Filtering DB 구현할 때, 기능에 따른 시스템 분리시 더욱 세부적으로 분류 가능하다.

Privacy 기반의 False-Positive 복구 기법은 S/W

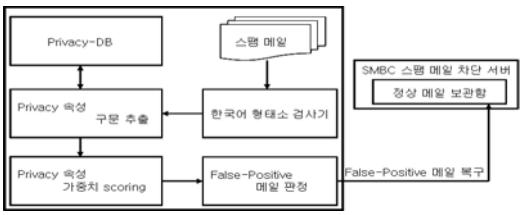

그림 6. False-Positive 메일 복구 처리 과정

의 복구 엔진으로 구성되어 임베디드 장치 내에서 False-Positive 메일 복구 처리와 결과에 따른 Privacy 추출 속성을 Privacy DB에 누적시킨다. 판정된 스팸 메일에 대한 결과는 메일 서버의 수신자 화이트 리스트(White List)에 추가하여, 추후 메일 송신 가능 여부를 판정하기 위한 Opt-Marker를 갱신한다.

서버형 차단 프레임에서 메일 서버에 스팸 메일 필터를 적용하므로, 기존의 스팸 메일 차단 서버는 메일 수신과 필터링에 대한 처리 부하가 매우 높다. 그러므로, 시스템 처리 부하를 분산시키기 위해 False-Positive 메일 복구 모듈은 물리적으로 독립된 스팸 메일 보관함에 적용하여 추가적인 작업의 처리 부담을 줄인다. 그리고 1개 이상의 False-Positive 메일의 복구는 스팸 메일 차단률 상승과 함께 신뢰성도 동시에 높이게 된다.

Ⅴ. 결론 및 향후 연구과제

본 논문에서는 스팸 메일 차단 필터가 발생시킨 False-Positive 메일을 복구하여, 차단 신뢰도를 향상시키기 위한 SMBC 플랫폼을 설계 및 제안하였다.

표 1. 성능 향상을 위한 기술 비교 분석

영역	항목	기존 차단 플랫폼[4,5,6]	SMBC 플랫폼	비교 분석
처리 능력	지식정보크기	높음	매우높음	- 상대적으로 방대한 스팸정보 - Privacy 정보 추가
	처리 복잡도	높음	매우높음	- Privacy 기반의 필터링 기술은 검사 유형이 유일하여 중복 적용 불필요
	처리 가속성	낮음	높음	- H/W 기반의 FA 적용에 따른 가속화 가능
	기능 확장성/이식성	높음	비교적 낮음	- 개인정보에 종속되어 확장/이식이 상대적으로 불리
	처리 안정성	보통	높음	- 작업 간소화 - FA를 통한 작업 분할 - 시스템 부가 감소
	비용	보통	매우 높음	- 독립된 시스템 유지 - 가속 H/W 추가
신뢰성	스팸 메일 복구	일부 가능	가능	- 스팸 메일 보관함 분리를 통한 추후 선택 복구 가능
	스팸 메일 차단	95%+ Filteration rate	기존 차단률+ Recovery rate	- 오인률 최소화에 따른 상대적 차단율 증가
	판정 오인	0.001% - 10%	기존 오인율-복구율	- 복구에 따른 판정 오인률 감소
	이용 신뢰도	보통	비교적 높음	- 차단율, 오인률 감소에 따른 시스템 신뢰도 증가

SMBC 플랫폼은 정상 메일 보관 장치와 스팸 메일 보관 장치를 분리시켜 시스템 처리의 부하를 줄이고, Privacy 기반의 False-Positive 메일 복구 기술의 적용을 통해 스팸 기반의 메일과 Privacy 기반의 메일 형식 모두 필터링하여 차단 신뢰도를 높였다.

표 1은 기존 스팸 메일 차단 시스템과 SMBC 플랫폼을 시스템 특성에 따라 비교 분석된 내용을 요약하고 있다. 처리 능력에 대한 항목별 비교에서 시스템 처리 가속성과 복구률, 차단 신뢰도는 구현 복잡도에 따라 처리 부하를 줄이기 위한 FA 가속기와 Privacy 기반의 False-Positive 메일 복구 기법 적용을 통해 기존의 차단 플랫폼보다 높은 처리 능력을 갖는다. 그러나, 참조되는 정보의 크기와 시스템의 복잡도, 비용적인 측면에서는 기존의 스팸 차단 플랫폼에 Privacy 기반의 복구 장치가 추가되어 낮은 처리 능력을 갖는다.

향후 연구 과제로 Privacy 기반의 스팸 메일 복구 기법을 차단 기법으로 변형시키고, 이를 기존의 스팸 메일 차단 필터와 대치하여 독립된 시스템 유지에 따른 복잡도 및 비용을 개선한다. 그리고, 더욱 정교한 한국어 구문 분석을 통해 Privacy 기반의 스팸 메일 복구의 정확도를 높이고, 이를 적용한 SMBC 플랫폼을 구현 및 성능 평가를 수행한다.

참 고 문 헌

[1] Aha. D.W., "A Study of Instance-Base Algorithms for Supervised Learning Task: Mathematical, Empirical, and Psychological Evaluations", *University of California, Irvine,* Technical Report 90-42, 1990

[2] Mehran Sahami, Susan Dumais, David Heckerman, Eric Horvitz, "A Bayesian Approach to Filtering Junk E-Mail", *AAAI*, TECHNICAL REPORT-AMERICAN ASSOCIATION FOR ARTIFICIAL INTELLIGENCE WS, Learning for text categorization, np, 55-62, 1998

[3] T. Saito, K. Umesawa, and H.G. Okuno, "A Privacy-Enhanced Access Control", *日本電子情報通信學會論文誌*, 2001. 11

[4] 김진만, 장종욱, "컨텐츠 필터를 이용한 스팸 메일 차단 시스템 설계 및 구현", *한국해양정보통신학회*, 2003년도 춘계 종합학술대회.

[5] 조한철, 조근식, "나이브 베이지안 분류자와 메시지 규칙을 이용한 스팸메일 필터링 시스템", *한국정보과학회*, 제29회 춘계학술대회, 2002.4.

[6] 하홍준, "기계학습을 이용한 내용기반 한국어 스팸메일 필터의 설계 및 구현", *건국대학교* 2003.2

[7] "이메일서비스 업체별 스팸메일 방지기술", *불법스팸대응센터*, 2002. 6

박 노 경 (Nho-Kyung Park) 종신회원

1984년 고려대학교 전자공학과 졸업
1990년 고려대학교 전자공학과 공학박사
1999년3월~2000년 2월 OSU ECE 연구교수
2005년3월~현재 차세대 반도체 연구소장
1988년~현재 호서대학교 전기정보통신공학부 정교수
<관심분야> HDTV, ASIC Design, SoC

한 성 호 (Sung-Ho Han) 정회원

1991년 호서대학교 정보통신공학과 공학석사 졸업
2005년 호서대학교 정보통신공학과 공학박사 졸업
2005년~현재 서울 호서전문학교 전임강사
<관심분야> SoC, DMB, ASIC Design

서 상 진 (Sang-Jin Seo) 정회원

1999년 부경대학교 전자계산학과 이학사 졸업
2001년 부경대학교 전자계산학과 이학석사 졸업
2001년~현재 서울 호서전문학교 모바일 미디어과 학과장
<관심분야> 임베디드 시스템, 멀티미디어 정보처리

진 현 준 (Hyun-Joon Jin) 정회원

1986년 고려대학교 전자공학과 공학석사 졸업
1998년 미국 리하이대학교 전산학 박사 졸업.
1998년~현재 호서대학교 전기정보통신공학부 부교수
<관심분야> 시스템 프로그램, 멀티미디어 정보처리