발송MTA의 재전송 기능을 이용한 동보 전송 스팸메일 차단 기법에 관한 연구

최명중° 황종선
고려대학교 컴퓨터공학과°
{kcmj77°, hwang}@korea.ac.kr

Research on the Method of Blocking Spam Mails Sent in the Form of Batch-Arrival by Resending Sender-MTA

Myung-Jung Choi°, Chong-Sun Hwang
Dept. of Computer Engineering, Korea University

요 약

인터넷의 급속한 성장으로 인터넷과 E-mail의 사용자가 증가하게 되면서, E-mail은 많은 사람들이 정보를 주고 받는 대표적인 통신수단의 하나로 자리 잡게 되었다. 그러나, 편리하고 비용이 거의 들지 않기 때문에 개인이나 업체들의 광고 수단으로 악용되고 있으며, 이에 따라 스팸 메일로 인한 시간과 비용의 낭비가 크게 증가하고 있다. 본 논문에서는 메시지 규칙에 기반을 둔 필터링 방식이 아닌 동보 전송 형태의 스팸 메일을 차단할 수 있는 방법을 연구한다.

1. 서 론

인터넷의 급속한 성장과 더불어 전자우편(E-mail)은 다른 매체들에 비하여 상대적으로 적은 비용으로 정보 및 의사 교환을 할 수 있는 장점 때문에 많은 사람들에게 중요한 통신 수단으로 인식되고 있다. 그러나, 편리하고 비용이 들지 않는 점을 이용해 많은 개인이나 업체들은 자신들의 상업적 광고를 무분별하게 발송하고 있으며, 그 양은 매년 폭발적으로 증가하고 있는 추세이다.[1] 이에 따라 메일 서비스 업체들은 저장 장치의 용량부족 등의 문제를 겪고 있으며, 일반 사용자들은 쏟아져 들어오는 상업성 광고 및 불법, 음란 광고로 인해 자신의 계정 부족 및 스팸 메일을 지우는데 시간을 투자하는 불편을 겪고 있다.[2]

스팸 메일에 대한 일반적인 정의를 살펴보면, 스팸 메일은 '발송자의 재화나 용역의 판매 촉진을 위한 상업적인(Commerial)인 내용으로 수신자가 원하지 않음에도(Unsolicited) 불구하고 불특정 다수에게 대량(Bulk)으로 전송되는 이메일'이라고 할 수 있다. 그러나 수신자가 원하는지, 원하지 않는지에 대한 판단과 상업성/대량성의 판단 기준이 구체적으로 명확하게 확립되지 않아 스팸 메일에 대한 판별은 쉬운 일이 아니다. 2004년 2월 19일 국내 IT 업체들에 따르면 지난해 국내에서 발송된 이메일 중 80~90%가 바이러스 메일 등을 포함한 스팸 메일로 집계됐다. 이는 스팸 메일 필터링 업체인 메시지랩스가 전 세계적 스팸 메일 비율로 밝힌 62.7%보다 훨씬 높은 수준이다.[3]

스팸 메일을 걸러내기 위한 방법으로 스팸 메일의 특징으로 대표될 수 있는 단어들을 찾아내는 메시지 규칙에 기반을 둔 필터링 방법을 주로 적용하지 있지만, 이런 방법만으로는 스팸 메일을 완벽히 걸러낼 수 없기 때문에 보다 효율적인 스팸 차단 방법을 제시한다.

본 논문은 구성은 다음과 같다. 2장에서 관련 연구, 3장에서 기존 메일 방식의 문제점 4장에서 재전송을 이용한 동보메일 형태의 필터링 기법 연구, 5장에서 본 논문의 결론과 향후 과제를 기술한다.

2. 관련 연구

스팸 메일을 걸러내기 위한 방법으로 대부분의 메일 시스템들은 메시지 규칙에 기반을 둔 필터링 방법을 주로 적용하고 있으며, 그 밖에 많은 확률적인 방법을 적용한 메일 필터링 시스템들이 개발되어 지고 있다. [4]

2.1 메시지 규칙을 이용한 분류

메시지 규칙을 이용한 필터링 방법은 스팸의 특징으로 대표될 수 있는 단어들을 찾아내어 스팸 메일의 여부를 판단하는 방법으로서 확률적인 방법들에 비해 단순하며 재현율과 정확도에 있어서도 비교적 좋은 성능을 얻을 수 있다.[5] 반면에 사용자가 직접 메시지 규칙을 입력해야 하며, 스팸 메일의형태가 변화함에 따라 메시지 규칙도 지속적으로 갱신시켜야 하는 문제가 발생한다. 뿐만 아니라 참과 거짓 두 가지의 경우만을 결과로 갖기 때문에 보다 정확한 필터링을 하는데 한계가 있다. [6]

2.2 나이브 베이지안 알고리즘

메일 필터링을 하는 과정에서 룰을 형성하고, 내용을 분류할 때 학습 알고리즘이 이용되며, 학습 알고리즘 중에서 베이지안 알고리즘이 가장 많이 사용되고 있다. 이 알고리즘은 모든 문서에서 특정 단어의 출현으로 구별되는 이진속성벡터(vector of binary attributes)로 표현된 모델로 문서를 정형화하는데, 모델은 다형성 베르누이 사건 모델(multi-variate Bernoulli event model)을 기초로 하여 각 카테고리의 문서마다 다르게 모델을 만들게 된다. 여기서

이용되는 가설은 문서들의 모든 속성은 주어진 전체 카테고리의 다른 문서의 전후 관계에 대해서 독립적이라는 것이다. 기본적인 알고리즘은 다음과 같다. 모델링 작업으로 만들어진 문서의 모델을 사용하여 각각의 카테고리별 문서의 확률 값 중 가장 높은 확률 값을 가진 카테고리에 문서를 분류하게 된다.[7]

2.3 스팸 메일에서의 특징 추출

가중치를 부여한 베이지안 분류자를 이용하여 스팸 메일 필터링을 하기 위해서는 우선 스팸 메일의 특징(Feature)을 추출(Extraction)해 내는 것이 중요하다. 단순한 나이브 베이지안 분류자의 경우 메일에서 공백(Space)으로 구분된 토큰(Token)들을 추출한 뒤, 그 토큰들의 출현 빈도수를 저장하고 이를 바탕으로 필터링이 가능하다. 하지만, 가중치가 부여된 베이지안 분류자에서는 스팸 메일에서의 특징을 추출해 놓아야만 적절한 요소들에 가중치를 부여함으로서 보다 정확한 필터링이 가능해지는 것이다.

2.3.1 이메일 헤더(E-Mail Header)

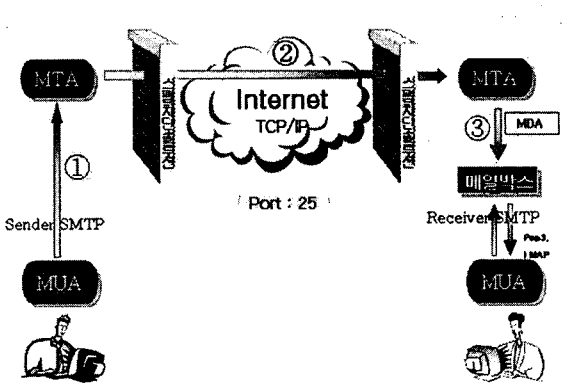
이메일을 주고받는 과정에서 메시지를 처리하는 서버는 제일 처음 메시지에서 자신이 작업을 처리하는데 필요한 헤더를 찾는다. 이 메시지 헤더의 정보는 사용자에 의해 직접 입력된 부분도 있으나, 메일/뉴스 프로그램 혹은 서버에 의해 자동으로 기록된 부분도 있다. 따라서, 이러한 이메일 헤더의 정보를 이용하여 스팸 메일의 여부를 판단하는데 사용할 수도 있다.

2.3.2. 메시지(Message)

이메일은 헤더 부분과 메시지 부분으로 이루어져 있다. 메시지 부분은 메일 발송자가 원하는 내용이 포함되는 부분이다. 메시지 부분에는 일반 텍스트와 HTML Tag가 주로 사용되는데, 메시지에 HTML Tag들과 같이 사용된 텍스트들을 관찰함으로서 스팸 메일의 여부를 판단할 수 있다. 즉, 스팸 메일에 자주 사용되는 특정 Tag들(<img src="">,<a href="">)과 같이 사용된 텍스트에 대해 가중치를 부여함으로서 스팸 여부를 보다 정확히 판단할 수 있게 된다.[8]

3. 기존 메일 방식의 문제점

(그림 1)은 수신자사서함 기반의 기존 메일방식에서 메일 소통을 보여주는데, 송신자가 발송한 메일은 수신메일서버에 있는 수신자 사서함에 보관된다. 메일 전달체계를 전체적으로 살펴보면 유무선 네트워크에 접속된 개인용 컴퓨터를 사용하여 메일을 작성하고 이를 송신메일서버로 보내는 송신자, 송신자가 작성하여 발송하도록 요청한 메일을 받아서 수신메일서버로 전달하는 송신메일서버, 송신메일서버로부터 메일을 받아서 수신자사서함에 저장하고, 수신자의 요청시 메일을 최종적으로 수신자에게 전해주는 수신메일서버, 그리고 수신측 메일 서버로부터 메일을 받아보는 수신자로 구성된다. 송신자가 송신메일서버로 메일을 전달하고(①)하고, 송신메일서버가 수신메일 서버로 메일을 전달(②)하는 통신 절차는 SMTP(Simple Mail Transfer Protocol)에 의해 수행되고, 수신메일서버에서 수신자가 메일을 읽어가는 통신절차는(③) IMAP(Internet Mail Access Protocol)나 POP3(Post Office Protocol)등에 의해 수행된다.



(그림 1) 기존 메일 방식

(그림 1)과 같은 메일소통 방식을 채택하는 기존 메일방식을 살펴보면 수신자의 의사와는 상관없이 송신자 임의대로 메일을 발송하여(①) 수신메일서버의 수신자사서함에 채워 넣는(②) 수신자사서함 기반의 구조적 특징으로 인해 다음과 같은 문제점이 초래된다. 메일 전달에 있어서 송신측은 별다른 부담이 없는 반면 수신측은 전달된 메일을 사서함에 보관해야 하고 보관된 메일을 읽어보거나 삭제해야 하는 등 메일 소통에 있어 부담을 지고 있다는 점이다. 그 결과 송신측에서 수신자가 원하지 않는 스팸메일이나 폭탄메일을 함부로 발송하는 등의 메일 사용에 있어 도덕적 해이가 만연하게 된다. 특히 스팸메일의 남발로 인해 메일 트래픽이 폭주하여 인터넷이 정체되고, 수신자 사서함이 스팸메일로 가득 차게 되어 사서함 공간의 낭비가 심각해주고, 수신측 메일 서버에 과부하가 걸려 필요한 메일의 소통에 큰 지장이 초래되는 등 많은 피해가 발생하고 있다.[9]

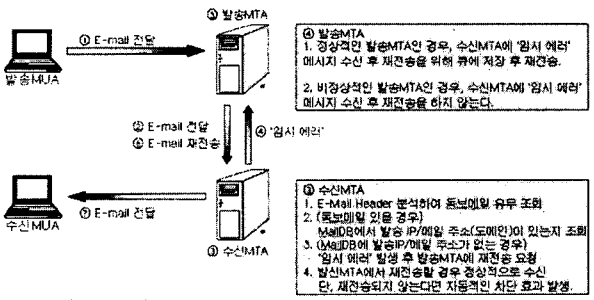
4. 동보전송 형태의 스팸 차단 기법 연구

기존의 필터링 방식이 수신MTA에 부하를 많이 발생시키므로, 수신MTA에 부하를 최소화시키면서 발송MTA에서 스팸 메일을 필터링 하는 방식을 제안하며, 그 중에서도 동보 전송 형태의 스팸 메일을 발송MTA 기반에서 필터링 하는 기법을 제안한다. 개념 및 동작 원리는 다음과 같다. 스팸 메일 필터링을 수신MTA가 아닌 발송

MTA에서 할 수 있도록 메일 수신시 다음과 같은 정보들을 추출하며, 이것을 "엔트리"라고 지칭한다.

a. 발송자 IP 주소
b. 발송자의 메일 주소(Envelop MAIL FROM: 주소)
c. 수신자의 메일 주소(Envelop RCPT TO: 주소)
d. 수신자의 메일 주소(E-Mail Header TO: 주소)
e. 수신자의 메일 주소(E-Mail Header CC: 주소)
f. 수신자의 메일 주소(E-Mail Header BCC: 주소)

이 6가지 정보는 메일 수신 서버에서 쉽게 수집할 수 있는 것으로, 이것이 수집되면 다음과 같은 조건을 적용시킨다. "RCPT TO, Header TO, CC, BCC에서 추출(③-1)된 '@' 개수가 4개 이상이(③-2)면서, 발송자 IP 주소 또는 발송자 메일 주소가 기존의 있던 정보가 아니라면, 수신 거부(③-3)를 한 후 일정 시간 동안 같은 발송자 IP 또는 발송자 메일 주소에서 수신되는 모든 메일을 거부한다. 거부 사유는 '임시에러(Temporary Failure)'으로 한다." 메일 프로토콜인 SMTP는 원래 불안한 네트워크에서 동작하도록 설계되었기 때문에, 메일 서버들은 '임시 에러' 메시지를 받게 되면, 일정한 시간 동안 재전송을 하도록 표준에 명기되어 있기 때문에, 정상적인 메일 서버라면 반드시 재전송(④-1)을 하게 될 것이다.[10]



(그림 2) 동보 메일 형태의 스팸 필터링 방법

일반적으로 스팸 발송자들은 스팸 발송만을 위한 전용 소프트웨어를 사용하기 때문에 발송 후 발송 기록을 저장하지 않는 특성이 있다. 정상 메일 서버들은 발송 대기 큐(Queue)에 저장해 뒀다가 일정 시간 후에 다시 재전송을 하는 "큐잉(Queueing)"을 수행하지만, 스팸 발송 프로그램 중 "큐잉(Queueing)"을 수행한 프로그램은 없다. "큐잉(Queueing)"이라는 것은 매우 복잡한 프로세스로서 스팸 발송자가 발송되지 않은 메일에 대해서 큐잉을 하게 되면 발송자의 발송큐에는 많은 수의 메일이 쌓여서 디스크에 많은 용량을 차지할 것이며, 스팸발송자가 큐잉을 하는 것은 비용적인 측면을 고려할 때 현실적으로 불가능하다. 하지만, 정상 메일 서버의 경우 어떤 큐잉 비용을 지불하고서라도 정상 메일을 전달해야 하는 의무가 있기 때문에, 큐잉이라는 절차가 복잡하고 무겁더라도 어쩔 수 없이 구현을 하여 사용할 수밖에 없다는 점에 착안하여 발송MTA의 재전송 기능을 이용한 동보전송 형태의 스팸 메일 차단 기법을 아래와 같이 제안한다. 이러한 방법은 수신MTA의 자원을 최소한으로 사용한다는 장점이 있으며, 발송IP/발송자 메일 주소만 저장하는 데이터베이스만 유지하면서 접속을 한번씩 더 해보는 정도의 부담 밖에 없다. 접속 후 수신자 주소까지만 받은 후 바로 차단하게 되므로 메일 본문까지 다 받은 후에 일일이 검사하는 스팸 차단 방법에 비해 처리할 데이터 양도 많이 감소되기 때문에 네트워크의 트래픽 및 내용을 점검하는 수신MTA의 부하도 감소하는 장점이 있다.

5. 결론 및 향후 연구과제

기존에 알고 있는 IP나 메일 주소가 아닌 경우, 동보 전송 형태의 스팸 메일을 무조건 '임시 에러'로 처리 후 발송MTA에 재전송을 요구하기 때문에, 스팸 메일의 차단 효과는 있지만, 재전송을 요구하기 때문에 '전달이 지연되는 현상'이 발생하는 문제점이 있으며, 향후 연구 과제에서는 '전달이 지연되는 현상'을 사용자가 거의 느낄 수 없는 지연 시간에 대한 실험 및 연구가 필요하다.

참고문헌

[1] 한국전산원, "국가정보화백서(National Informatization White Paper)", pp. 23, 2002.
[2] Inter E-mail Corporate Usage Report, www.securityman-agenment.com/library/worldtalk0200.html
[3] 김자경, 이광수 "스팸 메일 차단 방법론 비교분석", 한국정보과학회 가을 학술발표논문집, 2004.
[4] http://email.about.com/cs/bayesianspamsw/
[5] Diao, Y., Lu, H. and Wu, D., "A Comparative Study of Classification Based Personal E-mail Filtering," Technical report, Dept. of Computer Sciences at the U. of Texas ay Austin, 1999.
[6] Cohen, W.W., "Learning Rules that Classify E-Mail," Proc. Of the AAAI Spring Symposium on Machine Learning in Information Access, 1996.
[7] McCallum, A. Nigam, "A Comparison of Event Models for Naïve Bayes Text Calssification," In AAAI-98 Workshop on Learning for Text Categorization, 1998, http://www.cs.cmu.edu/~mccallum.
[8] 고수정, 이정현, "Apriori 알고리즘에 의한 연관단어 지식 베이스에 의한 가중치가 부여된 베이지안 자동문서 분류", 멀티미디어학회 논문지 제4권 제2호, 2001.
[9] 김태준, "송신자사서함 기반의 메일 방식에 관한 연구", 한국정보처리학회 논문지, 2004.
[10] RFC821, http://www.ietf.org/rfc/rfc0821.txt