UPVS를 이용한 스팸메일 차단시스템의 개발

안병태*, 김민선**
*가톨릭대학교 정보통신원
**협성대학교 유통경영학과
e-mail:ahnbt@catholic.ac.kr
e-mail: sunnyminkim@hanmail.net

A Development of Spam Mail Interception System using User Participation Verification System

Byeong-Tae Ahn*, Min Sun Kim**
*Information Communication Center, Catholic University
**Department of Distribution Management, Hyupsung University

요 약

전자우편(e-mail)은 매우 편리한 통신수단임에도 불구하고 무분별한 광고성 스팸메일(spam mail)의 침입과 타인의 메일을 가로채거나 변조가능성 등의 부작용 및 역기능으로 신뢰성에 문제가 되고 있다. 특히 기존의 스팸 방지 기술인 발송/수신 단계 스팸 방지 기술은 아직까지 스팸을 완벽하게 차단하지 못하고 있다. 따라서 본 논문에서는 기존의 스팸 방지 기술을 이용하여 1단계 차단을 거친 후 사용자 참여를 이용한 검증 시스템을 개발함으로써 스팸 차단 효율을 향상시키고자 한다.

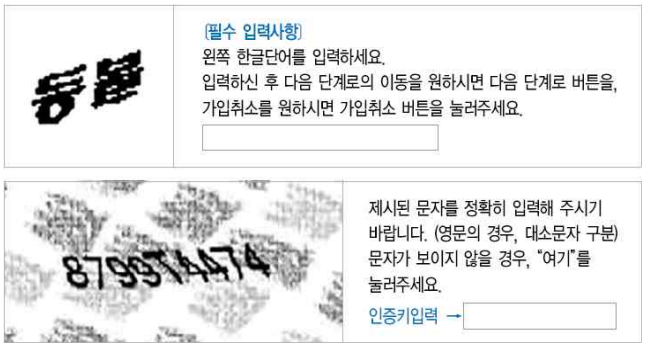
1. 서론

스팸메일이 사회문제로 등장한 것은 불과 7-8년 사이의 일이지만, 사회 전체에 미치는 영향력은 그 어떤 정보화 역기능보다 크고도 넓다. 네티즌 2000명을 대상으로 조사한 바에 따르면, 가장 피해를 입은 정보화 역기능으로 개인정보침해나 바이러스 피해보다 스팸메일을 꼽고 있다[1]. 물론 단일 피해 규모로는 개인정보침해나 바이러스 피해가 스팸메일로 인한 것보다 크겠지만, 스팸메일은 일상적이고 보다 대중적으로 발생하는 피해이기 때문이다. 가장 일반적인 스팸메일 차단 방법으로는 스팸 메일의 제목이나 내용에 존재하는 특정 단어나 보낸 사람을 이용하여 차단하는 방법이 있으며, 대부분의 웹 메일이나 메일 클라이언트에서 이를 지원한다. 그러나 이와 스팸메일이라고 규정지을 수 있는 단어나 보낸 사람에 대한 정의가 쉽지 않고 계속적으로 변하는 스팸메일에는 적용하기가 힘든 단점이 있다. 그리고 기존의 스팸 차단 기술은 기계적인 시스템이기 때문에 아직까지 스팸 메일을 완벽하게 차단할 수 있는 시스템은 존재하지 않는다. 따라서 본 논문에서는 이와 같은 문제점을 해결하기 위해 1차적으로 기존의 스팸 차단 기술을 사용하면서 기존의 기술로 차단하지 못하는 스팸에 대해 2차적으로 사용자 참여를 이용한 검증 시스템(UPVS)을 거쳐 최종적으로 스팸 차단 효율을 향상시키고자 한다. 2장 관련연구에서는 최근 스팸 메일 방지 기술에 대해 알아보고 3장에서는 사용자 참여 검증 시스템을 통한 스팸 메일 차단 방법을 개발한다. 끝으로, 4장에서는 결론 및 향후과제를 제시한다.

2. 관련 연구

스팸 메일 방지 기술에는 발송 단계 스팸 방지 기술, 수신 단계 스팸 방지 기술, 메일 주소 수집 차단 기술, 메일 주소 자동 생성 대응 기술, 웹 메일 자동 등록 차단 기술 등이 있다. 발송 단계 스팸 방지 기술은 인터넷을 통해 통과하는 모든 메일의 통신 채널인 25번 포트를 차단하여 ISP가 구현한 스팸 방지 대응방법을 적용한 기술이다[2]. 수신 단계 스팸 방지 기술은 수신측 메일 서버가 발송 측 메일 서버의 과거 신뢰도에 근거하여 어떤 것이 스팸이고 어떤 것이 스팸이 아닌지를 결정하는 것이다[3]. 본 필터링 기술에는 수신 허용(화이트) 리스트와 수신

거부(블랙) 리스트가 있으며 이를 통해 스팸 메일을 차단하는 기술이다. 본 차단 기술은 수신측 메일 서버가 발송측 메일 서버의 과거 신뢰도에 근거하여 어떤 것이 스팸이고 스팸이 아닌지를 결정하는 시스템 기술이다[4]. 메일 주소 수집 차단 기술은 스팸메일을 보내는 스패머가 메일 주소를 홈페이지에서 자동으로 수집 못하도록 여러 형태로 변환시키는 기술이다. 메일 주소 자동 생성 대응 기술은 스패머가 메일 주소를 생성하여 메일을 방송할 때 메일 서버가 존재하지 않는 메일 주소에 대해서 '수신자 없음' 확인 메일을 확인해 주지 않도록 설정하는 기술이다. 따라서 메일 주소가 실재 존재 하는지 존재하지 않는지 판별할 수가 없다. 웹 메일 자동 등록 차단 기술은 회원 가입 단계에서 HIP 기술을 적용함으로써 자동 프로그램에 의한 무차별적인 계정 생성을 제한한다. 대표적인 예로 단순한 단어를 무작위로 골라 글자를 약간 훼손시킨 뒤 복잡한 배경 화면 위에 표시하는 CAPTCHA(Completely Automated Public Turing test to tell Computers and Humans Apart) 방법이 있다[5]. [그림 1]은 CAPTCHA 기술 예시를 나타낸 것이다.



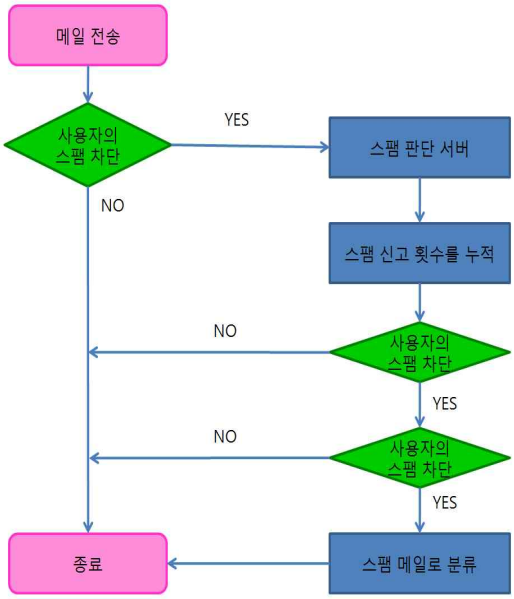
[그림 1] CAPTCHA(Completely Automated Public Turing test to tell Computers and Humans Apart)

3. UPVS를 이용한 스팸 메일 차단 시스템

본 논문에서는 1차적으로 기존의 스팸 차단 기술을 사용하고 기존의 기술로 차단하지 못하는 스팸에 대해 2차적으로 사용자 참여를 이용한 검증 시스템(UPVS)을 이용하여 최종적으로 스팸 차단 효율을 높인다.

3.1 UPVS 시스템 흐름도

[그림 2]는 UPVS 시스템을 이용한 스팸 차단 흐름도를 나타낸 것이다.



[그림 2] UPVS 시스템 흐름도

[그림 2]는 메일이 사용자에게 발송된 후 사용자가 스팸 메일이라는 판단을 하면 스팸 판단 서버에 스팸 신고를 한다. 스팸 판단 서버는 일정한 규칙에 따라 판단을 하여 해당 메일에 대한 사용자의 스팸 신고 횟수를 누적한다. 누적된 스팸 신고 횟수가 1차 기준선을 넘을 경우 DB 서버에 저장되어 있는 해당 메일의 총 회수를 파악한다. 그리고 누적된 스팸 신고 횟수가 2차 기준선을 넘을 경우 스팸 메일이라고 판단하여 DB 서버에 저장되어 있는 해당 메일 중 아직 사용자가 읽지 않은 메일을 스팸 메일로 분류하게 된다. 위와 같이 메일서버에서 동일한 메일들을 파악하고 이 메일을 읽은 사용자가 일정한 수준(예를 들면, 해당메일의 20%라던가 아니면 절대적인 수로 200명)이 해당 메일을 스팸으로 인식할 경우 그 메일을 읽지 않은 사용자의 계정에서 해당 메일을 스팸메시지로 처리하도록 한다. 이에 따라 메일을 읽지 않은 사용자의 경우에는 스팸으로 분류 되지 않았던 메일이 다른 사용자의 판단에 의하여 스팸으로 새롭게 분류가 된다. 따라서 본 스팸 메일 차단 시스템은 사용자의 판단능력을 다수의 사용자가 공유하여 차단하는 기술이다. 기존의 스팸 차단 기술이 사용자의 패턴이나 행동을 파악하지 못했다면 이 기술은 다수의 사용자가 다른 사용자의 판단을 함께 공유하는 것이 된다.

3.2 UPVS 가상 구현

[그림 3]은 UPVS 스팸 메일 차단 시스템 구성도를 나타낸 것이다.

[그림 3] UPVS 시스템 구성도

[그림 3]은 1차적으로 스팸 분류가 이루어져도 필터링이 제대로 이루어지지 않은 메일이 일반 메일함에 존재할 가능성이 있다. 따라서 메일함에는 필터링 되지 않은 스팸 메일이 존재한다. 스팸 감지기는 1차적으로 분류된 메일 중 가입자가 스팸으로 신고한 메일의 제목과 내용을 전송받아 스팸 DB에 저장하고 신고 회수를 카운트 한다. 신고 횟수가 정해진 기준을 넘으면 읽지 않은 해당 메일을 일반 메일함에서 스팸 메일함으로 이동시킨다. 스팸 DB는 사용자가 스팸으로 신고한 메일의 제목과 내용을 저장하며 신고 횟수에 대한 카운트를 저장한 후 일정 시간이 지난 메일은 DB에서 삭제되도록 한다.

4. 결론 및 향후과제

본 논문에서는 사용자가 아직 읽지 않은 메일에 대해 검증 시스템의 정보를 활용하여 다시 한 번 스팸을 검출하는 UPVS를 이용한 스팸 메일 차단 시스템을 개발하였다. UPVS를 이용한 스팸 메일 차단 시스템은 기존의 스팸 방지 기술을 보완할 수 있으며 따로 스팸 메일로 신고하지 않더라도 자동으로 스팸 메일로 신고 된다.

향후 과제로는 스팸으로 판단하는 기준 개수를 정하는 것이기 어렵고 적정한 수준으로 정하지 않을 경우 차단 효율이 떨어지거나 스팸이 아닌 메일을 스팸으로 처리할 수 있는 부작용이 발생한다. 따라서 이를 방지하기 위해 사용자 참여율을 높여 차단 효율성을 높이고 스팸 메일만 차단이 되도록 해야 할 것이다. 그리고 스팸 메일 차단 검증 시스템 구동 중 시스템의 과부하가 발생하지 않도록 검증 시스템의 효과적인 전처리기가 필요하다.

참고문헌

[1] Muhammad N. Marsono, M. Watheq EI-Kharashi and Fayez Gebali. "Targeting spam control on middleboxes: Spam detection based on layer-3 e-mail content classification," Computer Networks, Volume 53, No 6, 23 April 2009, pp. 835-848.

[2] Kuo-Ching Ying, Shih-Wei Lin, Zne-Jung Lee and Yen-Tim, "An ensemble approach applied to classify spam e-mails," Expert Systems with Applications, Volume 37, No 3, 15 March 2010, pp. 2197-2201.

[3] 최홍식, 김중환, “PGP를 이용한 스팸메일 차단 시스템의 개발,” 한국정보보호학회 논문지, 제 14권 제 6호, pp. 135-148, 12월, 2004.

[4] 백기영, 이철수, 류재철, “URL 빈도분석을 이용한 스팸메일 차단 방법,” 가톨릭대학교 종합포털 정보시스템 최종보고서, 2008. 11.

[5] “웹사이트에서의 전자우편주소 추출방지 기술 개발”, 한국정보보호진흥원, 2002. 12.