Journal of the Korean Data Analysis Society, Vol. 7, No. 4, August 2005, pp. 1487-1494

스팸메일 필터링 시스템에 대한 실증연구

신양규[1]

요 약

본 연구에서는 전자메일이 대표적인 통신수단이 됨에 따라 최근 사회적 문제가 되고 있는 스팸메일에 대한 대처방안과 관련하여 기업 및 공공기관에서 도입하는 스팸메일 필터링시스템의 효율성에 대하여 살펴보고자 한다. 초고속 인터넷 및 컴퓨터의 급속한 발달에 따라 전자메일의 수와 사이즈가 급증하고 있다. 효율적이고 편리한 통신수단인 전자메일의 유용성을 역이용하여 스패머들이 엄청난 양의 스팸메일을 전송하고 있는데 이는 메일트래픽을 가중시킬 뿐 아니라 사회적, 경제적으로 큰 문제를 일으키고 있다. 본 연구에서는 스팸메일을 차단하고 관리하기 위해 개발되고 있는 스팸메일 필터링시스템의 효율성을 실증적으로 검증하고자한다.

주요용어 : 스팸메일, 스팸필터, 필터링기법, 스팸메일 필터링시스템.

1. 서론

초고속 인터넷의 보급에 비례하여 전자메일의 수 및 사이즈가 증가하고 있다. 이는 메일서버의 부하를 증가시켜 메일트래픽을 발생시키고 나아가 메일수신의 지연 및 수신 불능 등의 현상을 초래하여 메일서버에 대한 업그레이드를 요구하게 되는데, 메일시스템에 대한 하드웨어적인 투자증가는 한계가 있다.

메일트래픽을 증가시키는 가장 큰 잠재적 위협 요소는 스팸메일이다. 스팸메일은 인터넷 사용자들에게 원하지도 않았는데 무작위로 발송되는 광고성 전자메일에 대한 통칭으로 Bulk메일, Junk 메일, Unsolicited메일이 모두 유사한 의미로 사용된다(Cranor and Lamacchia, 1998). 스팸메일은 그 내용이 최근 들어 광고성 메일에서부터 음란성 메일에 이르기까지 매우 광범위한데 수신자들의 대부분이 그 내용에 관심이 없을 뿐 아니라 메일 사용자들에게 시간 낭비와 정신적 피해를 초래 할 수 있고 메일 시스템 관리 측면에서는 메일 서버에 과부하 등을 초래하여 경제적인 손실을 야기 시킨다. ISP 업체인 UUNet은 스팸퇴치를 위해 연간 12억원의 예산을 들여 6명으로 구성된 팀을 운영하고 있으며(Internet Week, 1998), Netcom의 경우에는 고객이 지불하는 금액의 10%가 스팸메일 처리에 따른 비용이라고 한다(New York Times, 1998). 그리고 유럽 연합 보고서에 따르면 유럽 내의 메일트래픽의 70% 이상을 스팸메일이 차지하고 있다고 한다(BlackSpider Technologies, 2004). 한국정보보호진흥원(2003)의 자료에 의하면 우리나라에서도 1인당 하루 스팸메일 수신이 2001년 약 5통,

[1]712-715 경상북도 경산시 유곡동 290번지, 대구한의대학교 자산운용과학과 교수. E-mail : yks@dhu.ac.kr

2002년 약 35통, 2003년 약 40통으로 2003년 6월 우리나라 6세 이상 국민의 64.1%가 인터넷을 보유하고 있고 이중 84.6%가 전자메일을 보유하고 있다는 한국인터넷정보센터의 정보화실태조사를 기준으로 하면 1년간 국내에서 유통되는 총 스팸메일의 양은 약 3천억 통으로 추산할 수 있다(한국인터넷정보센터, 2003; 한국통신문화재단, 2003). 정보통신부에서는 스팸메일 관련 상담 및 불법 스팸신고를 처리하기 위하여 2003년 1월 24일 한국정보보호진흥원내에 불법스팸대응센터(www.spamcop.or.kr)를 개설하였고 스팸메일 차단프로그램을 개설 배포하는 등의 기술적인 대책 마련에도 주력하고 있다. Kim(2005)은 효율적 정보보호를 위한 ID와 Password에 대한 분석을 하였다. 그러나 전반적으로 스팸메일을 규제하기 위한 법적인 노력은 스패머의 발송기술이 갈수록 지능화되면서 지금까지 큰 효과를 거두지 못하고 있다.

스팸메일 차단을 위한 가장 기본적인 방법인 메일 수신자가 스팸메일에 대해 일일이 수신거부를 하고 스패머의 도메인주소를 추적하는 것인데 이는 대부분의 수신자들에 있어서 거의 불가능에 가까우므로 적극적으로 대응을 하지 못하고 있다. 좀더 효과적인 방법은 메일 수신자가 도구프로그램을 사용하여 자신에게 전달된 메일을 검사하여 스팸메일을 자동으로 확인하고 삭제하도록 하는 것이다. 기업이나 공공 기관의 경우에는 스팸메일 관리시스템을 도입하는 것이 효과적이다. 자동으로 메일을 검사하여 스팸메일을 관리하는 프로그램을 스팸필터라고 하는데 사용되는 기법은 스패머들에 대한 블랙리스트를 이용하는 기법에서부터 메일 내용을 분석하여 스팸메일 여부를 판단하는 내용기반기법에 이르기까지 다양하다. 최근에는 스팸메일 필터링을 위해 RBL(Realtime Blocking List)을 이용하고 있다. 이는 실시간으로 스팸메일을 발송하거나 위험요소가 존재하는 사이트의 목록을 메일서버에 적용시켜 스팸메일을 차단하는 것이다. 스팸메일의 분류 및 차단은 서버레벨, 네트워크구조레벨 그리고 메일 수신자레벨에서 관리 할 수 있는데 본 연구에서는 서버레벨 차원에서 스팸메일을 차단하고 관리하는 스팸메일 차단시스템의 효율성에 대하여 살펴보고자 한다.

2장에서는 서버레벨에서의 스팸메일 필터링기법에 대해 살펴보았고, 3장에서는 스팸메일 시스템으로 메일을 필터링한 결과를 제시하고 이를 분석하였다. 마지막으로 스팸메일 필터링시스템도입의 효율성에 대하여 논하였다.

2. 서버레벨에서의 스팸메일 필터링기법

필터링원리는 누군가가 해당도메인으로 메일을 발송하면 서버에 메일이 도착하기 전에 필터링 서버에서 스팸메일 유무를 판단하여 스팸메일로 판단된 메일을 걸러내는 것이다. 시스템 증설, 운영인력충원에 따른 추가적인 투자비용을 절감시켜주고 안정적인 메일서비스를 보장하기 위해서는 메일 서버의 전방에서 스팸/바이러스 메일을 지능적으로 처리하고 메일트래픽을 효율적으로 관리하는 것이 필요하다.

메일서버레벨에서 스팸메일 관리시 예상되는 문제점으로는 스팸메일/바이러스메일의 처리규칙

생성방법, DOS(Denial of Service) 공격, SMTP(Simple Mail Transfer Protocol) 공격에 대한 대응을 생각 할 수 있다. 스팸메일을 차단하기 위해서는 먼저 메일서버로 유입되는 메일을 스팸메일과 정상메일로 분류하여야 하는데 스패머들이 스팸을 어떻게 만들어 낼지를 예측하기에는 쉬운 일이 아니지만 기존의 스팸메일의 패턴을 분석하여 유추할 수 있다. 자료의 분류방법 및 패턴 분석에 대한 연구는 통계학적으로 다양하게 이루어지고 있다. Kim(2003) 은 데이터마이닝에서의 분류방법에 대하여 연구하였고, Choi, Kim, Kang Cho and Son(2001), 그리고 Kang and Han(2003) 은 웹로그 데이터를 분석하여 온라인 사용자의 패턴을 분석하는 연구를 하였다. 메일의 자동분류에 대한 연구는 지금까지 여러 사람들에 의해 다양하게 이루어지고 있다. Ruvini and Gabriel(2002), Mock(2003), Giorgetti and Sebastiani(2003) 그리고 Manco, Macciari, Ruffolo and Tagarelli(2003)은 일반적인 문서분류기법을 이용한 스팸메일 필터링기법에 대한 연구를 하였으며 P. Graham(2002)은 베이지안 분류기법을 이용한 스팸메일 필터링기법을 제시하였고 Robinson(2003a, 2003b)은 Graham이 제안한 방법에서 문제점으로 제시된 희소단어처리, 단어의 발생빈도 반영 등에 대한 문제점을 일부 해결한 방법을 제시하였다. 베이지안 기법은 Graham(2002)이 논문에서도 밝혔듯이 현재까지 일반적인 문서분류기법을 이용한 스팸메일필터보다 학습에 의해 개인에 특화된 규칙을 스스로 만들어 내는 베이지안 기법을 이용한 스팸필터의 효율성이 더 높은 것으로 평가되고 있다. 다양한 스팸메일 유형에 대응 가능한 차단율이 높은 스팸메일필터시스템을 구현하기 위해서는 여러 가지 필터링기법을 복합적으로 사용하는 것이 효율적이다.

현재 많이 이용하고 있는 전자메일서비스제공업체들이 서버레벨에서 스팸방지를 위해 사용하고 있는 방법은 다양한 필터링기법활용 및 스팸신고란 운영이다(한국정보보호진흥원, 2003). 한국정보보호진흥원의 “메일서비스업체별 스팸방지 기술”보고서에 의하면 다음, 야후, 드림위즈, 라이코스, 코리아닷컴, 한미르 그리고 MSN등 현재 가장 많이 이용하고 있는 전자메일 서비스업체에서 제공하는 서버 차원에서의 스팸메일 필터링 단계는 수신차단 주소지정/특정조건필터링/기타 자사 고유한 필터링방법이다. 즉 기본적으로 서비스업체별로 필터링 수준을 정하여 발신자, 수신자, 참조, 제목이나 내용의 단어 등의 특정조건 필터링을 제공해 주고 메일 수신자가 수신차단주소나 도메인을 지정하여 원하지 않는 메일을 차단하는 것이다

3장. 실증분석

본 연구에서 스팸메일 필터링시스템의 효율성을 검증하기 위하여 사용한 필터링엔진은 테라스테크놀로지의 Terrace Mail Watcher이다. Terrace Mail Watcher에서 제공하는 스팸필터링 및 차단기법은 세 단계에 걸쳐 7종류의 필터에 의한 다중구조이다. Connection 단계, Contents 단계, User 단계의 세 단계로 설정된 필터링 규칙을 가진 Terrace Mail Watcher는 첫 번째 단계인 Connection 단계에서는 대량 스팸처리를 두 번째 단계인 Contents 단계에서는 불법 스팸차단을 하고 있다. 각 단계별로 사용되고 있는 필터링 기법은 살펴보면 Connection 단계에서는 과다발송 스패머 동작 차단

필터, SMTP 필터가 Contents 단계에서는 Pattern Matching 필터, Heuristic AI 필터, 표준감시 필터, 바이러스필터가 User 단계에서는 사용자 필터를 이용하여 스팸처리를 한다. 각 단계별로 베이지안 필터링 기법이 적용되어 대상 그룹에 적합한 필터링 기준을 생성하고 있다.

테스트 기간은 2004년 12월 15일에서 28일까지 2주 동안이고 테스트 대상은 대구한의대학교 전자메일 사용자 전체에게 수신되는 메일이고 사용된 서버 OS는 RedHat Linus ES이다.

다음 <표 1>는 일별 메일 필터링 결과에 대한 요약이다.

<표 1> 메일 필터링 일별 통계

	12.15	12.16	12.17	12.18	12.19	12.20	12.21
정상 메일	945	2,838	2,803	2,728	1,496	2,299	2,545
스팸 메일	12,537	45,427	45,181	44,826	34,784	42,584	40,424
바이러스 메일	23	106	130	85	49	136	147
일별 통계	13,505	48,371	48,114	47,639	36,329	45,019	42,137
	12.22	12.23	12.24	12.25	12.26	12.27	12.28
정상 메일	2,449	3,518	3,354	1,256	1,265	2,041	2,254
스팸 메일	38,934	41,825	44,739	24,647	31,080	49,260	53,069
바이러스 메일	150	143	154	61	54	139	142
일별 통계	42,137	45,486	48,247	25,964	32,399	51,440	55,465

<표 1>에 의하면 테스트 기간동안 처리된 총 메일 수는 593,419 건인데 이중 정상메일은 31,791 건으로 전체의 5.4%에 불과한 반면 스팸메일이 549,317건으로 92.6%, 바이러스메일이 1519건으로 0.2%를 차지하고 있음을 알 수 있다. 메일 사용자 1인당 하루 평균 수신하는 20건의 메일 중 정상메일은 한 건밖에 없다고 할 정도로 스팸메일의 양이 엄청나므로 스팸메일 차단에 대한 대책이 필요하다고 할 수 있다. 전체 메일 수신량의 90% 이상을 차지하는 스팸메일을 차단하고 처리함으로써 메일서버의 부하율이 1/3이하로 감소됨을 예상할 수 있다. 또 하루 4 만여 건의 스팸메일을 차단시 연간 1억 원 정도의 시스템비용(망 사용료 및 스토리지 비용 포함)절감을 기대할 수 있다. 인건비 면에서도 메일 사용자 일일 평균 20여건의 스팸메일의 처리로 인한 인적비용의 절감을 예측할 수 있다. 스팸메일의 처리시간을 메일 1 건당 평균 5 초 소요될 것으로 예상할 때 메일사용자 일인당 시간당 노무비를 1만원으로 하여 전체 메일 사용자 2000명을 대상으로 산정 하면 연간 약 2억 원의 인적비용 절감을 예상 할 수 있다.

다음 <표 2>는 스팸메일을 그룹별로 분류한 것이다.

<표 2>에 의하면 549,317건의 스팸메일 중 금융관련(Financial) 스팸메일이 204,389건으로 전체의 37.2%를, Spamrobat 엔진에 의해 차단되는 것이 130,957건으로 전체의 23.8%로 상품홍보, 광고관련이 113,886건으로 전체의 20.7%를 차지한다. 그러므로 정규표현식에 의해 규칙을 등록하면 효율성 있는 필터링체계를 구성 할 수 있다(예를 들면 \ [| \ { | \ (| \ * | # | - | < | : | \ |).*광.*고.*(\ ] | \ } | \ ) | \ * | # | - | > | : | \ |).

<표 2> 스팸메일 그룹별 분류

	12.15	12.16	12.17	12.18	12.19	12.2	12.21
mtasystem Financial	4,988	15,556	15,981	17,671	13,194	15,599	15,650
mtasystem spamrobot	1,481	10,403	7,389	7,329	9,455	10,617	12,796
mtasystem Product	1,660	6,740	7,408	5,558	4,097	3,912	3,935
mtasystem kwanggo_sample	730	4,459	4,510	2,214	919	4,489	3,428
mtasystem Education	989	2,541	2,511	5,091	4,101	3,563	1,673
mtasystem Health	1,954	3,951	5,613	5,880	1,519	2,826	1,166
mtasystem Fraud	126	790	747	614	641	296	319
mtasystem BAD_Format	35	68	101	38	34	41	365
mtasystem Spam_Subject	302	14	16	1	197	716	878
mtasystem Adult	85	608	549	130	123	255	173
TOTAL	12,537	45,427	45,181	44,826	34,784	42,584	40,424

	12.22	12.23	12.24	12.25	12.26	12.27	12.28
mtasystem Financial	11,267	14,379	16,912	11,166	12,866	16,287	22,873
mtasystem spamrobot	11,045	10,947	10,875	6,172	7,798	11,548	13,102
mtasystem Product	5,408	3,849	5,876	2,921	3,876	6,533	5,966
mtasystem kwanggo_sample	4,625	4,747	4,373	839	2,163	5,448	3,205
mtasystem Education	4,093	4,319	4,878	1,826	1,796	4,782	3,175
mtasystem Health	670	908	123	101	1,286	2,523	2,658
mtasystem Fraud	688	709	496	575	284	386	700
mtasystem BAD_Format	653	730	915	773	627	664	375
mtasystem Spam_Subject	325	1,090	90	84	222	635	484
mtasystem Adult	142	120	92	145	105	326	378
TOTAL	38,934	41,825	44,739	24,647	31,080	49,260	53,069

4. 결론

3장의 스팸메일 필터링시스템 테스트 결과에 의하면 스팸메일은 네트워크 장애 및 인적, 물적 자원낭비를 초래 할 수 있으며 나아가 업무환경저해와 정신적 스트레스를 일으킬 수 있다. 즉 여러 측면에서 많은 문제점들을 일으키고 있음을 알 수 있다. 특히 바이러스메일은 스팸메일에 비해 양은 많지 않지만 바이러스의 특성상 그 숫자에 관계없이 유입될 시에 네트워크부하 증가, 사용자 데이터의 유실 및 시스템의 오 작동 및 과부하를 일으킬 수 있으므로 강력한 대책이 필요한 메일이다. 스팸메일 필터링시스템을 도입하면 바이러스메일의 차단도 가능하므로 스팸메일 시스템의 도입은 스팸/바이러스메일의 차단 및 관리를 통하여 정상메일만이 전달되게 함으로써 정상메일의 확인이 신속하게 이루어지게 하여 업무효율을 증대시키고 더불어 메일관리시스템도입 및 네트워크 관리비용을 절감할 수 있다. 스팸메일 필터링시스템의 도입과 관련되는 문제점으로는 날로 다양해져 가는 스패머들의 스팸 생성 방법으로 인해 스팸메일을 효과적으로 차단하기 어려운 점과, 일괄처리로 인해 발생할 수 있는 유용한 메일차단의 위험성 즉 정상메일을 스팸메일로 판단하여 필터링 해 버릴 수 있다는 점이다. 베이지안 필터링기법은 개개마다 필터링 규칙이 다르고, 이 규칙도 시간에 따라 변화하므로 스패머들이 대응하기에 어려운 점이 많으므로 날로 지능화 되어 가는 스

패머들의 공격은 베이지안 필터링기법을 사용하면 어느 정도 해결이 가능하다고 할 수 있다. 그러나 베이지안 필터링기법도 수신된 스팸메일을 토대로 한 사후적 대책임을 감안한다면 현실적으로 서버레벨에서 스팸메일을 완벽하게 차단한다는 것은 불가능하다. 따라서 서버레벨에서의 스팸메일 차단시스템의 효율적 사용과 함께 네트워크구조레벨 그리고 메일 수신자레벨에서 적극적으로 스팸메일을 차단하여 스팸메일로 인한 피해를 최소화하는 것이 바람직하다.

참고문헌

[1] 한국인터넷정보센터 (2003). *정보화실태조사*.

[2] 한국정보보호진흥원 (2003). *메일서비스업체별 스팸방지 기술*. URL: www.spamcop.or.kr

[3] 한국통신문화재단 (2003). *우리집 스팸메일 추방교육운동*.

[4] BlackSpider Technologies (2004). *A Buyers Guide to Spam Filtering*.

[5] Choi, S. B., Kim, K. K., Kang, C. W., Cho, S. K. and Son, J. K. (2001). A study on the Comparison of Web Log Analyzers, *Journal of the Korean Data Analysis Society,* Vol. 4, No. 2, 327-340.

[6] Cranor, L. F. and Lamacchia, B. A. (1998). *Spam!, Communications of the ACM,* Vol. 41, No. 8, 74-83.

[7] D. Giorgetti and F. Sebastiani (2003). Automating Survey Coding by Multiclass Text Categorization Techniques, *Journal of American Society for Information Science and Technology,* Vol. 54, 1269-1277.

[8] G. Manco, E. Macciari, M. Ruffolo and A. Tagarelli (2003). *Towards an Adaptive Mail Classifier,* Technical report, ISI-CNR.

[9] Gary Robinson (2003). *Spam Detection*. URL: www.radio.weblogs.com/0101454/categories/spam/

[10] Gary Robinson article in the Linux Journal march 2003 issue 107. URL: www.linuxjournal.com/article.php?sid=6467

[11] Internet Week, May 4, 1998. CMP Media Inc, Manhasset, New York.

[12] J. Ruvini and J. Gabriel (2002). *Do Users Tollerate Errors from their Assistant?,* Experiments with an E-mail Classifier, IUI'02.

[13] Kang, H. C. and Han, S. T. (2003). A Clustering Algorithm for the Classification of Web Usage Patterns, *Journal of the Korean Data Analysis Society,* Vol. 5, No. 2, 337-344.

[14] Kim, K. K. (2003). A Study on Classification Methods in Data Mining, *Journal of the Korean Data Analysis Society,* Vol. 5, No. 1, 101-112.

[15] K. Mock (2001). *An Experimental Framework for Email Categorization and Management,* SIGIR '01.

[16] Kim, U. S. (2005). Research about ID and Password for efficient information protection, *Journal of the Korean Data Analysis Society,* Vol. 7, No. 1, 297-304.

[17] New York Times, March 19, 1998.

[18] Paul Graham (2002). *A Plan for Spam* . URL: www.paulgraham.com/spam.html

[2005년 6월 접수, 2005년 8월 채택]

A Study for Prevention of Spam-Mail Filtering System

Yang Kyu Shin[1]

Abstract

This study examines the efficiency of the spam-mail filtering system adopted by companies and public institutes as a response to the spam-mail problem which has become a social issue since electronic mails have been utilized as major communication devices. The rapid improvement of high-speed internet and computer is triggering the growth of electronic mail both in number and size. Spamers avail of the efficiency and convenience of electronic mails to produce huge amounts of spam-mails leading to not only "mail traffic" but also social and economic problems. This is an empirical study on the efficiency of the spam-mail filtering systems that are being developed to quarantine and administer spam-mails.

Keywords : Spam-mail, Spam filter, Filtering method, Filtering system.

[1]Professor, Department of Asset Management, Haany University, Yugok-dong, Gyeongsan-si, Gyeongsangbuk-do 712-715, Korea. E-mail : yks@dhu.ac.kr