스팸메일 차단을 위해 IP 주소간 거리 측정 알고리즘을 이용하는 전자우편 발송서버의 권한확인 방법

임 호 성[†] · 심 재 홍[††] · 최 경 희[†††] · 정 기 현[††††]

요 약

본 논문에서는 스팸메일을 차단하기 위해 전자우편 발송서버가 발신자가 소속된 도메인에 등록된 서버인지 또는 그 도메인에 속한 서버인지 판단하는 IP 주소간 거리 측정 알고리즘을 이용하는 전자우편 발송서버 권한확인 방법을 제안한다. 제안 방법은 전자우편을 발송한 서버의 IP 주소와 전자우편의 발신자 도메인의 DNS에 등록된 IP 주소들과의 거리를 이용해 전자우편을 발송한 서버가 전자우편의 발신자 도메인의 네트워크에 존재하는지 확인하여 스팸메일을 차단한다. 일정기간 동안 수집한 전자우편에 대해 제안 알고리즘을 적용하여 IP 주소간 거리를 측정한 결과 정상메일의 경우 88%, 스팸메일의 경우 10% 정도가 발신자가 소속된 도메인에 속한 전자우편 서버에서 발송되었고, 나머지는 발신자 주소를 도용하였거나 또는 제3의 장소에 존재하는 서버에서 발송하였음을 확인하였다. 제안 알고리즘은 발신자 도메인이 전자우편 발송 권한을 부여하지 않은 서버로부터 수신된 전자우편을 모두 스팸메일로 간주하여 스팸메일을 차단하는데 독립적으로 사용될 수 있으며, 또한 현재 표준화가 진행 중인 전자우편 발송서버 권한확인 프로토콜들이 보편화되어 사용되기 전까지 이들 프로토콜의 보완책으로도 사용될 수 있다.

키워드 : 스팸 메일, 전자우편 발송서버의 권한 확인 기법

E-mail Sending-Server Authorization Method using a Distance Estimation Algorithm between IP Addresses for Filtering Spam

Hosung Yim[†] · Jaehong Shim[††] · Kyunghee Choi[†††] · Gihyun Jung[††††]

ABSTRACT

In this paper, we propose E-mail sending-server authorization method using a distance estimation algorithm between IP addresses to check whether the E-mail sending server is registered in the domain of mail sending server or belongs to the domain for filtering spam mail. This method utilizes the distance between the IP address of sending server and IP addresses registered in the DNS to figure out that the E-mail sending server exists in the domain to filter spam mail. The experimental result of applying the proposed algorithm to sample E-mails gathered in a large size laboratory says that 88 percents of legitimate E-mails and only 10 percents of spam mails are sent by servers in the same domains of senders. The algorithm may be effectively used to block spam mails sent by servers outside of the domains of mail senders. It may be also hired as a temporary E-mail protecting system until the standard E-mail authorization protocol is fully deployed.

Key Words : Spam Mail, An Authorization Mechanism For E-mail Sending Server

1. 서 론

전자우편은 다른 통신수단보다 송수신 비용이 저렴하고 빠르기 때문에 많은 사람들이 이를 활용하고 있으며 대표적인 통신수단으로 자리매김 하고 있다. 그러나 이러한 전자우편 특성으로 인해 광고를 위해 전자우편을 사용하는 사업자들이 점점 늘어나고 있다. 이처럼 광고를 위해 대량으로 발송되는 전자우편을 스팸(spam)메일이라 한다. 스팸메일은 불법적인 광고를 포함하고 있어 사용자를 불쾌하게 만들거나 허가 없이 사용자의 전자우편 계정 용량을 차지한다[1]. 스팸메일에 대한 국가적인 법 제재에도 불구하고 아직도 많은 스팸메일이 사용자들에게 발송되고 있다.

현재 스팸메일을 차단하기 위한 다양한 연구들이 진행되고 있다. 전자우편의 어떤 부분을 통해 스팸 유무를 결정할 것인가에 대한 관점에서 스팸메일 차단 기법은 크게 세가지로 나눌 수 있다[2, 3]. 첫째, 전자우편의 제목 및 본문 등 내용을 기반으로 스팸메일을 차단하는 기법이다. 이것은 정규 표현식 혹은 간단한 단어 검색을 이용해 스팸메일을 찾아내고 차단

† 준 회 원 : 아주대학교 정보통신전문대학원 석사과정
†† 정 회 원 : 조선대학교 인터넷소프트웨어공학부 교수
††† 정 회 원 : 아주대학교 정보통신전문대학원 교수
†††† 정 회 원 : 아주대학교 전자공학부 교수
논문접수 : 2004년 12월 22일, 심사완료 : 2005년 5월 3일

한다. 그러나 이 기법은 새로운 스팸메일의 패턴이 생길 때마다 새로운 정규 표현식이나 검색 단어를 주기적으로 추가하여야 하며, 정규 표현식이 많을 경우 스팸메일 차단에 상당한 시간을 필요로 하게 된다. 또한 문자열을 기반으로 검색하기 때문에 HTML 문서를 통해 이미지만 보여주는 스팸메일의 경우에는 차단하기 힘들다. 인공지능 기법을 이용한 전자우편 분류방법 역시 전자우편의 내용을 기반으로 한다[4, 5]. 이 방법은 문자열 검색이나 정규 표현식을 이용한 스팸 차단 방법보다는 사용자가 설정해야 하는 초기 입력 데이터는 적지만, 이것 역시 문자열을 기반으로 하기 때문에 HTML을 사용해 이미지만 보여주는 스팸메일일 경우 차단하기 힘들다.

둘째, 발신자 전자우편 주소를 기반으로 블랙 리스트(black list), 혹은 화이트 리스트(white list)를 구성하여 스팸메일을 차단하는 기법이다[2]. 이 기법은 전자우편이 서버에 들어오기 전에 차단하는 효과가 있지만, SMTP 상에서 발신자 주소를 얼마든지 조작할 수 있기 때문에 스팸메일을 차단하기 어렵고, 또한 사용자가 직접 화이트 리스트 및 블랙 리스트를 관리해야 하는 불편함이 있다. 이 불편함을 해소하기 위해 발신자 확인 전자우편 시스템이 제시되었으나, 메일링 리스트에 대한 처리가 미흡하고 발신자 확인을 위해 생성되는 전자우편 개수가 많으며, 또한 SMTP 상에서 사용되는 발신자의 전자우편 주소가 조작될 경우 잘못 전달되는 전자우편이 생길 수 있다는 단점을 가지고 있다[6].

마지막 기법은 RBL(real-time black hole list) 혹은 ORBL (open RBL) 등과 같은 블랙 리스팅(blacklisting) 기법이다[2]. 이 기법은 특정 기관에서 공개하는 스팸메일을 자주 보내는 발신자의 IP 주소 리스트 및 도메인 리스트를 이용해 스팸을 차단한다. 그러나 최근의 스팸메일 경향을 보면 발신자의 IP 주소 및 도메인을 바꿔가며 사용하기 때문에 이 기법 역시 큰 효과를 보지 못 한다[7].

위와 같은 전자우편 차단 기법 이외에도 스팸메일 발송자가 웹(web)을 통해 전자우편 주소를 수집하는 것을 원천적으로 봉쇄하는 기법이 있다. 그러나 이 방법은 새로이 생성되는 전자우편 주소에 대해서만 스팸메일 수신을 막을 수 있다는 단점을 가진다[8]. 또 다른 기법으로 수신자의 전자우편 주소를 고정하지 않고 유동적으로 변경하여, 수신자의 전자우편 주소로 곧바로 오는 전자우편은 수신하지 않고 유동적으로 변경된 전자우편 주소로 들어오는 전자우편만을 수신하는 방법이 있다[9]. 이 기법은 전자우편을 보내는 사람이 유동적으로 변경되는 전자우편 주소를 일일이 찾아봐야 하는 단점을 가지고 있기 때문에 사용하기 힘들다.

최근의 스팸메일들은 발신자의 전자우편 주소를 조작하는 경우가 많다[7]. 이 경우 발신자 전자우편 주소를 이용해 블랙 리스트나 화이트 리스트를 구축하는 스팸 차단 기법은 무용지물이 된다. 그리고 발신자 확인 시스템의 경우 조작된 발신자 전자우편 주소로 확인 전자우편이 배달되어 실제 발신자 전자우편 주소를 사용하는 사용자에게는 스팸이나 다를 바 없게 된다[6]. 이는 SMTP 설계 시 스팸메일에 대한 고려가 이루어지지 않았기 때문이며, 이로 인해 발신자 주소 조작이 가능하게 된 것이다. 스팸메일의 영향이 점점 커지자 발신자의 전자우편 주소 조작을 방지하기 위해 SMTP를 기반으로 전자우편 발신자를 인증하는 방법에 대한 연구가 활발히 진행되고 있다. 그 결과로 RMX(Reverse MX)[7], Caller ID [10], SPF(Sender Policy Framework)[11], SCAF(Simple Caller Authentication Framework)[12]와 같은 전자우편 발송서버의 권한확인 프로토콜들이 제시되었고, 현재 표준화가 진행 중이다. 이러한 프로토콜들은 발신자 주소 중 도메인에 대한 조작을 막는 방법을 제시하고 있다. 하지만 이 방법들은 표준화가 진행 중에 있고 보편화 되어 사용되기 전까지는 사용에 제약이 따른다. 즉, 특정 도메인이 이러한 프로토콜들을 채택하고 있지 않을 경우, 발신자 전자우편 주소가 소속된 도메인에 전자우편 발송서버가 실제로 존재하는지를 판단할 수 있는 방법이 필요하다.

본 연구에서는 이러한 방법을 제시하고 이를 활용할 수 있는 방안에 대해 논의한다. 일반적으로 전자우편 수신 시 해당 전자우편 발신자의 전자우편 주소가 소속된 도메인의 DNS 서버와 접속하여, 해당 DNS에 등록된 DNS 정보, 즉 MX (mail exchange) 리소스 레코드, A(address) 리소스 레코드, NS(name server) 리소스 레코드에 저장된 IP 주소들을 발췌할 수 있다. 본 논문에서는 해당 DNS 서버에서 발췌한 IP 주소들과 실제 전자우편을 전송한 발송서버의 IP 주소와의 IP 주소간 거리를 측정하는 알고리즘을 제안한다. 일정기간 수집된 실제 전자우편에 대해 제안된 알고리즘을 적용하여 측정한 IP 주소간 거리를 분석하고, 이를 바탕으로 정상메일과 스팸메일을 구분하는데 제안 알고리즘을 활용 가능하다는 것을 확인하였다. 또한 현재 표준화가 진행 중인 전자우편 발송서버의 권한확인 프로토콜들이 널리 활용되기 전까지 이러한 프로토콜들을 사용하지 않는 도메인에 대해 전자우편 발송서버가 발신자의 전자우편 주소상의 도메인 내에 실제로 존재하는가를 판단할 수 있는 기법으로 본 연구에서 제안하는 알고리즘을 활용 할 수 있다.

본 논문의 구성은 다음과 같다. 2절에서는 전자우편 발송서버와 발신자 도메인과의 상관관계를 알아본다. 3절에서는 IP 주소간 거리 측정을 통한 전자우편 발송서버 권한확인 기법을 제안하며 기법에서 사용되는 IP 주소간 거리측정 알고리즘을 제시한다. 4절에서는 제안된 IP 주소간 거리측정 알고리즘을 적용하여 측정한 IP 주소간 거리를 바탕으로 정상메일과 스팸메일에서의 IP 주소간 거리를 분석하고, 분석 결과를 토대로 제안 알고리즘의 활용방안을 제시한다. 마지막 5절에서 본 연구의 결론 및 향후 연구에 대해 기술한다.

2. 전자우편 발송서버와 발신자 도메인과의 상관관계

본 절에서는 전자우편 발송서버의 IP 주소와 발신자가 소속된 도메인과의 상관관계를 분석하고, 스팸메일과 정상메일의 차이점을 도출하고자 한다. 이를 위해 본 연구에서는 한 기관에서 사용자들의 허가를 얻어 일정기간 동안 총 48,842개의 전자우편에서 실험에 필요한 정보만을 발췌하였다. 수집된

전자우편 중 15%인 7,259개만 정상메일이고, 나머지 85%인 41,583개는 스팸메일이었다. 정상메일과 스팸메일은 전자우편 제목과 전자우편 내용의 일부를 직접 확인하여 분류하였으며, 정상메일에 비해 스팸메일이 5배 이상 더 많았다.

<표 1>은 정상메일과 스팸메일에 대해 전자우편의 개수에 따라 발신자가 소속된 상위 10개의 도메인을 보여준다. 도메인들 중 hanmail.net과 empal.com은 정상메일 및 스팸메일 모두에 포함된다. 스팸메일은 모두 전자우편 서비스를 하고 있는 포털 사이트의 도메인이 사용되고 있다.

〈표 1〉 수집한 전자우편 중 상위 10개의 발신자 도메인

발신자 도메인	정상메일 개수	발신자 도메인	스팸메일 개수
hanmail.net	388	hotmail.com	3698
sciencetimes.co.kr	203	yahoo.com	3567
emsmail.naver.com	186	yahoo.co.kr	3304
goodmail.hani.co.kr	162	hanmail.net	2813
bioneer.co.kr	151	empal.com	1364
em4s.com	130	msn.com	789
imas.cjmall.com	90	naver.com	778
donga.com	89	freechal.com	766
joins.com	88	netian.com	668
empal.com	81	korea.com	516
기타 (1116개 도메인)	5691	기타 (7552개 도메인)	23320

〈표 2〉 정상메일 중 상위 6개의 도메인에 대한 발송서버가 소속된 네트워크의 IP 주소

발신자 도메인	네트워크 IP 주소 (발송서버 개수)	메일 개수	발신자 도메인	네트워크 IP 주소 (발송서버 개수)	메일 개수
hanmail.net	211.43.197.0 (11)	377	goodmail.hani.co.kr	211.233.22.0 (2)	162
	211.172.254.0(1)	6			
	211.115.65.0(1)	3			
	61.0.0.0(1)	1			
	203.226.253.0 (1)	1			
sciencetimes.co.kr	211.40.179.0 (1)	202	bioneer.co.kr	61.0.0.0 (1)	151
	210.107.239.0 (1)	1			
emsmail.naver.com	211.218.151.0 (3)	114	em4s.com	211.189.120.0 (7)	128
	211.218.150.0 (1)	72		210.107.239.0 (1)	2

<표 2>는 정상메일 중 전자우편을 많이 발송한 상위 6개의 도메인에 대해 전자우편 발송서버가 소속된 네트워크의 IP 주소를 보여준다. 정상메일의 경우 거의 같은 네트워크에서 전자우편이 발송되었으며, 두 개 이상의 다른 네트워크로부터 전자우편이 발송된 경우도 있으나 이것은 릴레이를 통해 들어온 전자우편으로 확인 되었다. hanmail.net 도메인에서는 다른 도메인과 달리 많은 네트워크에서 메일이 발송된 것을 볼 수 있다. hanmail.net은 메일 서비스를 하는 포털 도메인으로 양질의 메일 서비스를 위해 메일 서버를 여러 곳으로 분산시켜 놓은 것으로 확인되었으며, 마지막 203.226.253.0 네트워크에서 발송된 메일은 릴레이를 통해 들어온 메일이었다. emsmail.naver.com 도메인에서는 비슷한 두 네트워크에서 전자우편이 수신되었는데, 확인 결과 이것은 전자우편 발송서버가 실제로 두 네트워크에 분리되어 있었다.

<표 3>은 스팸메일 중 상위 4개의 발신자 도메인에 대한 발송서버가 소속된 네트워크의 IP 주소를 보여준다. 스팸메일의 경우 같은 발신자 도메인이라 할지라도 상당히 많은 수의 서로 다른 네트워크에서 전자우편이 발송되었다. 이는 곧 여러 개의 서로 다른 네트워크에서 일반적으로 널리 사용되는 포털 사이트의 도메인을 도용하여 스팸메일을 발송했다는 것을 알 수 있다.

〈표 3〉 스팸메일 중 상위 4개의 도메인에 대한 발송서버가 소속된 네트워크의 IP 주소

발신자 도메인	네트워크 IP 주소 (발송서버 개수)	메일 개수	발신자 도메인	네트워크 IP 주소 (발송서버 개수)	메일 개수
hotmail.com	61.0.0.0 (85)	506	yahoo.co.kr	221.154.16.0 (24)	784
	64.0.0.0 (211)	419		222.100.31.0 (15)	386
	218.146.13.0 (2)	333		61.0.0.0 (24)	369
	211.216.136.0 (2)	257		210.102.36.0 (1)	164
	65.0.0.0 (176)	176		203.240.242.0 (1)	135
	외 400개의 네트워크 (639)	2007		외 216개의 네트워크 (252)	1466
yahoo.com	220.78.42.0 (28)	475	hanmail.net	61.0.0.0 (130)	412
	221.151.249.0 (3)	381		221.138.65.0 (1)	168
	220.88.93.0 (29)	358		210.216.220.0 (1)	149
	222.117.215.0 (37)	353		203.234.177.0 (1)	118
	61.0.0.0 (46)	201		220.86.69.0 (1)	108
	외 395개의 네트워크 (893)	1799		외 417개의 네트워크 (457)	1858

<표 4>는 정상메일을 많이 보낸 상위 10개의 발송서버가 전송한 전자우편에 대한 발신자 도메인의 통계를 보여준다. 거의 모든 발송서버가 동일한 도메인을 가진 전자우편만을 발송하고 있는 것을 알 수 있다. 즉, 각각의 발송서버는 해당 도메인에 등록된 합법적인 전자우편 발송서버임을 짐작할 수 있다.

<표 5>는 스팸메일에 대해 상위 4개의 발송서버가 전송한 전자우편에 대한 발신자 도메인의 통계를 보여준다. 하나의 발송서버에서 다양한 도메인을 가진 스팸메일들을 전송한다는 것을 알 수 있다. 이는 곧 전자우편 발송서버가 릴레이 서버이거나 또는 특정 도메인에 속하지 않은 임의의 발송서버에서 전자우편의 발신자 도메인을 조작해 대량의 전자우편을 발송했음을 의미한다.

〈표 4〉 정상메일을 전송한 상위 10개의 발송서버가 전송한 전자우편의 발신자 도메인

발송서버 IP 주소	발신자 도메인	전자우편 개수	발송서버 IP 주소	발신자 도메인	전자우편 개수
211.40.179.15	sciencetimes.co.kr	202	218.145.68.114	joins.com	87
61.85.113.10	bioneer.co.kr	151	210.182.119.91	kyobobook.co.kr	81
64.125.132.240	subversion.tigris.org	78	218.145.56.59	mailer.hunet.co.kr	73
	tortoisesvn.tigris.org	31			
211.233.22.184	goodmail.hani.co.kr	108	211.218.150.106	emsmail.naver.com	72
210.115.150.66	donga.com	88	211.116.129.21	kics.or.kr	60

<표 3>과 <표 5>를 통해 스팸메일의 경우, 다수의 네트워크에 산재해 있는 전자우편 발송서버에서 동일한 포털 사이트의 도메인을 도용하거나, 또는 임의의 서버에서 발신자 도메인을 기존의 여러 포털 사이트로 위조해 대량으로 스팸

메일을 보내고 있음을 알 수 있다. 따라서 본 연구에서는 정상메일과 스팸메일의 이러한 특성 차이를 활용해 이들을 분류할 수 있는 알고리즘을 제안하고, 실험을 통해 제안 알고리즘의 타당성을 보이고자 한다.

〈표 5〉 스팸메일을 전송한 상위 4개의 발송서버가 전송한 전자우편의 발신자 도메인

발송서버 IP 주소	발신자 도메인	전자우편 개수	발송서버 IP 주소	발신자 도메인	전자우편 개수
220.86.69.36	hanmail.net	108	220.78.178.142	hanmail.net	28
	hitel.net	74		mail90.tt.co.kr	21
	hotmail.com	53		kyungwon.ac.kr	14
	yahoo.com	34		mju.ac.kr	14
	soback.kornet21.net	32		haksan.dsc.ac.kr	12
	외 10개 도메인	255		외 93개 도메인	187
211.177.6.176	hanmail.net	76	222.108.72.31	netian.com	165
	hitel.net	61		unitel.co.kr	65
	hotmail.com	43		dreamwiz.com	34
	yahoo.com	29		esab.seah.co.kr	10
	soback.kornet21.net	26			
	외 10개 도메인	170			

3. IP 주소간 거리 측정 알고리즘

IP 주소는 인터넷 상에서 한 기기를 지칭하기 위해 사용되는 32bit의 주소이다. IP 주소는 네트워크 주소와 호스트 주소로 나뉘는데 네트워크 주소에 따라 A, B, C, D, E 클래스 주소로 나뉜다. D는 멀티캐스트를 위해 준비되어 있는 주소이며, E 클래스는 예약되어 있는 주소이다. 따라서 실제 인터넷에서 하나의 기기를 지칭하기 위해서는 A, B, C 클래스의 주소를 사용해야 한다. IP 주소를 32bit의 이진수로 표현할 경우 사람이 인지하기 어렵기 때문에, 일반적으로 사람이 인지하기 쉽도록 202.30.31.35와 같은 형식으로 8bit씩 나누어 표현한다.

일반적으로 IP 주소간 거리라고 하면 RIP의 거리 벡터(distance vector) 알고리즘에서 사용하는 두 호스트 사이의 라우터 개수라고 볼 수 있다[13]. 하지만 두 호스트간의 존재하는 라우터의 개수는 제 삼자가 측정하기 어렵기 때문에, 본 논문에서는 IP 주소상의 거리를 두 IP 주소 값의 차이를 상대적 크기로 표현한다. 즉, 두 IP 주소가 얼마나 다른가에 따라 얼마나 멀리 떨어져 있느냐를 판단한다.

IP 주소간 거리 측정을 통한 전자우편 발송서버의 권한확인 절차는 (그림 1)과 같다. 먼저 SMTP를 통해 전자우편을 수신하고 해당 전자우편을 전송한 발송서버의 IP 주소를 확보한다. 그리고 전자우편 발신자의 전자우편 주소가 속해있는 도메인의 DNS와 접속하여 등록된 DNS 정보, 즉 MX(mail exchange), A(address), NS(name server) 리소스 레코드에 저장된 서버들의 IP 주소를 발췌한다. IP 주소간 거리 측정 알고리즘을 통해 DNS에서 발췌된 IP 주소와 전자우편 발송서버의 IP 주소간 거리를 측정한다. DNS에 등록된 각 서버와 발송서버와의 IP 주소간 거리를 측정한 후, 그 중 가장 작은 값을 최종 측정 값으로 택한다. 측정된 거리를 바탕으로발신자 도메인이 전자우편 발송서버에게 전자우편 발송 권한

```
IPorig = 수신된 전자우편의 발송서버 IP 주소;
DNS = 수신된 전자우편의 발신자 주소가 소속된 도메인 이름 시스템;
IPList = Get_IPList(DNS, A, MX, NS);
            /* DNS의 A, MX, NS 리소스 레코드에 명시되어 있는
            IP 주소 리스트를 발췌한다. */

MinDistance = 5;                    /* 최대 IP 주소간 거리 */
FOR EACH IP IN IPList {
   Dist = BaiscIPDistance(IPorig, IP);
                    /* 기본 IP 주소간 거리 측정 알고리즘 */
            or
   Dist = ClassIPDistance(IPorig, IP);
                /* 클래스 기반 IP 주소간 거리 측정 알고리즘 */
   IF (Dist < MinDistance)
       MinDistance = Dist;
}

IF (MinDistance > Threshold) {
                    /* Threshold : 관리자에 의해 설정 됨 */
    전자우편 발송서버가 권한을 가지고 있지 않음;
    수신한 전자우편을 스팸으로 분류;
} Else {
    전자우편 발송서버가 권한을 가지고 있음;
    수신한 전자우편을 정상으로 분류;
}
```

(그림 1) IP 주소간 거리를 이용한 전자우편 발송서버의 권한확인 절차

을 부여했는지를 결정한다. 이는 측정된 거리가 사전에 시스템 관리자에 의해 정의된 임계치 보다 적으면 발송서버는 전자우편 발송권한이 있는 것으로 판단한다. 만약 권한이 없는 서버일 경우에는 수신된 전자우편을 스팸메일로 분류한다.

본 논문에서는 IP 주소간 거리 측정을 위해 기본 IP 주소간 거리 측정 알고리즘과 클래스(class) 기반 IP 주소간 거리 측정 알고리즘을 제안한다. IP 주소간 거리를 측정할 때 두 IP 주소가 동일한 IP 주소인지, 아니면 동일한 네트워크에 포함된 주소인지에 따라 서로 의미하는 바가 달라진다. 전자의 경우 서로 다른 IP 주소를 가지고 있을 경우 거리가 멀게 나올 수 있지만, 후자의 경우 서로 다른 IP 주소를 가지고 있더라도 동일한 네트워크에 포함되어 있으면 두 IP 주소는 매우 가깝다라고 할 수 있다.

3.1 기본 IP 주소간 거리 측정 알고리즘

(그림 2)는 기본 IP 주소간 거리 측정 알고리즘으로 IP 주소를 바이트 단위로 4개의 바이트로 나눈 후 각각을 비교하는 알고리즘으로 얼마나 동일한 IP 주소를 가지고 있는지에 대한 측정을 한다.

(그림 2)의 알고리즘을 이용하면 두 IP 주소간 거리는 0부터 4까지 나타날 수 있다. 0이 가장 가까운 거리에 있는 것을 의미하고, 4는 가장 먼 거리에 있는 것을 의미한다. 거리 0은 두 IP 주소가 동일하다는 것을 의미한다. 거리 1은 두 IP 주소의 처음 세 자리는 같고 끝자리 하나만 다른 경우이고, 거리 2는 앞의 두 자리는 같지만 세 자리부터 다른 경우, 거리 3은 앞의 한 자리만 같고 두 자리부터 다른 경우, 거리 4는 첫 자리부터 다르다는 것을 의미한다.

이 알고리즘의 장점은 IP 주소간 거리를 비교적 정확하게 측정할 수 있다는 것이다. 하지만, 두 IP 주소가 동일한지만 판단할 수 있고 두 IP 주소가 같은 네트워크에 있더라도 거

리가 0이 아닌 1, 2, 3의 값을 가질 수 있다는 단점을 가지고 있다. 이 단점을 보완하기 위해서는 IP 주소의 클래스를 통해 같은 네트워크에 있는지, 다른 네트워크에 존재하는가를 측정해야 한다.

```
FUNCTION BasicIPDistance(IP1, IP2)
{
  /* IP1, IP2는 바이트 단위로 네 부분으로 구분된 배열이라 가정함 */
  FOR i = 0 TO 3 {
     IF (IP1[i] != IP2[i]) THEN RETURN 4-I;
  }
  RETURN 0;
}
```

(그림 2) 기본 IP 주소간 거리 측정 알고리즘

3.2 클래스(class) 기반 IP 주소간 거리 측정 알고리즘

전자우편 발송서버가 비록 등록된 서버와는 다른 서버일지라도 동일한 도메인에 소속되어 있는 네트워크에 존재하는 서버일 경우, 이 서버로부터 발송된 전자우편은 정상메일로 간주할 수 있다. (그림 3)의 클래스(class) 기반 IP 주소간 거리 측정 알고리즘은 두 IP 주소가 같은 네트워크에 있는가 그렇지 않으면 얼마나 떨어져 있는 네트워크에 존재하는가를 측정하는 알고리즘이다.

```
FUNCTION ClassIPDistance(IP1, IP2) {
  /* IP1, IP2는 바이트 단위로 네 부분으로 구분된 배열이라 가정함 */
  IF (0 < IP1[0] < 128) THEN Range = 0; /* A 클래스 IP 주소 */
  ELSE IF (128 <= IP[0] < 192) THEN Range = 1;
                                  /* B 클래스 IP 주소 */
  ELSE Range = 2;                 /* C 클래스 IP 주소 */
  FOR i = 0 TO Range {
      IF (IP1[i] != IP2[i]) THEN RETURN 4-i;
  }
  RETURN 0;
}
```

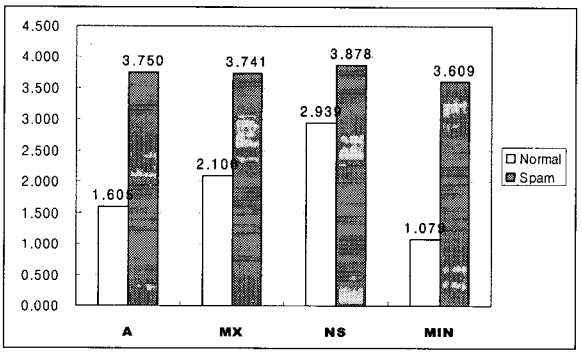
(그림 3) 클래스 기반 IP 주소간 거리 측정 알고리즘

(그림 3)의 알고리즘을 사용할 경우 두 IP 주소간 거리 역시 0부터 4까지 나타날 수 있다. 거리가 0이라는 것은 두 IP 주소가 동일하거나 또는 비록 IP 주소는 다를지라도 동일한 도메인 또는 지역 네트워크에 소속되어 있다는 것을 의미한다. 그 외에 클래스 C는 거리 2~4, 클래스 B는 3~4, 클래스 A는 4 범위 내의 거리가 존재할 수 있다. 이 알고리즘은 두 IP 주소가 같은 네트워크에 포함되는가, 아니면 다른 네트워크에 존재하는가를 검사할 수 있는 장점을 가지고 있지만, 현재 인터넷은 클래스에 의해 구분되는 네트워크를 서브넷을 이용해 한번 더 나누기 때문에 정확한 네트워크 구분을 할 수 없는 단점이 있다. 하지만 IP 주소가 어떤 서브넷에 있는가를 정확하게 측정하는 것은 어려울지라도 어떤 클래스에 있는가를 검사하는 것은 용이하기 때문에 이 알고리즘을 IP 주소간 거리 측정에 사용하도록 한다.

4. IP 주소간 거리 측정 및 분석

본 절에서는 앞 절에서 제안한 IP 주소간 거리 측정 알고리즘을 이용하여 실제 전자우편을 발송한 서버와 발신자 전자우편 주소가 소속된 도메인의 DNS에 등록된 서버들과의 IP 주소간 거리를 측정하고, 정상메일과 스팸메일의 IP 주소간 거리를 비교 분석해 본다. 실험에 사용된 전자우편들은 이미 2절에서 사용된 총 48,842개의 사용자의 동의를 얻어 수집된 전자우편들이다.

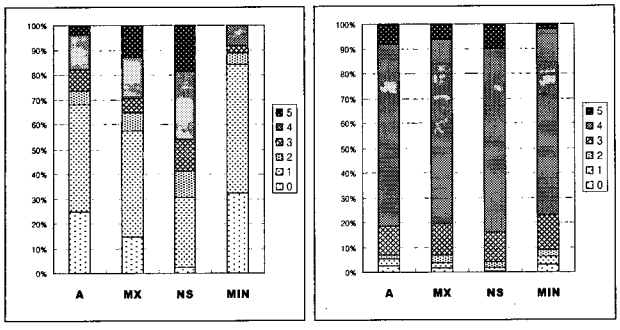
실험에서 전자우편 발신자 도메인의 DNS 서버에 등록된 DNS 정보, 즉 MX, A, NS 리소스 레코드에 저장된 IP 주소들을 발췌하여, 실제 전자우편을 전송한 발송서버 IP 주소와의 IP 주소간 거리를 측정하였다. 각 리소스 레코드별로 등록된 IP 주소와의 거리를 측정했으며, 리소스 레코드에 등록된 IP 주소들이 여러 개 일 경우 각각에 대해 거리를 측정한 후 가장 짧은 거리를 택했다. 그리고 각 MX, A, NS 리소스 레코드별로 가장 짧은 거리를 구한 후 이들 중 가장 짧은 거리는 MIN으로 나타내었다. 거리 측정 시 해당 도메인에 대한 DNS 정보가 없거나 또는 해당 리소스 레코드에 대해 등록된 IP 주소가 없을 경우 IP 주소간 거리를 5로 설정하였다.



(그림 4) 기본 거리 측정 알고리즘을 이용한 평균 IP 주소간 거리

(그림 4)는 기본 IP 주소간 거리 측정 알고리즘을 이용하여 측정한 IP 주소간 평균 거리를 보여주고 있다. 그림은 각 리소스 레코드별로 정상메일과 스팸메일의 전체 평균 거리를 보여 준다. 그림에서 정상메일은 전자우편 발송서버의 IP 주소가 A 리소스 레코드에 등록된 서버의 IP 주소와 가장 많이 일치하거나 가까우며, 그 다음으로 MX, NS 리소스 레코드에 등록된 서버 순으로 평균 IP 주소 거리가 점점 멀어지고 있다. MIN의 경우 거의 1에 가까운 IP 주소간 거리를 보인다. 그러나 스팸메일인 경우 리소스 레코드에 상관없이 모두 평균 거리가 거의 4에 가깝다. 전자우편 발송서버와 발신자 도메인의 DNS에 등록된 서버들과의 IP 주소간 평균 거리를 통해 정상메일과 스팸메일의 평균 거리가 확연히 차이가 난다는 것을 쉽게 인지할 수 있다.

(그림 5)는 정상메일과 스팸메일에 대해 각 리소스 레코드별로 기본 거리 측정 알고리즘을 이용하여 측정한 IP 주소간 거리들의 백분율 분포를 보여 준다. 그림의 MIN에서 정상메일의 경우 88% 정도가 0에서 2의 IP 주소간 거리를 보이고 있으나, 스팸메일인 경우 90% 이상이 3 이상의 거리를 보이고 있다. 이는 정상메일을 발송한 대부분의 서버들은 해당 도메인에 등록된 서버(거리 0)이거나 도메인에 등록된 서버들과 거리가 가깝다(거리 1~2)는 것을 의미한다. 그러나 스팸메일



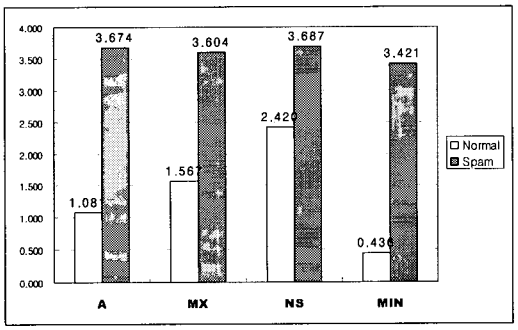
(a) 정상메일 (b) 스팸메일

(그림 5) 기본 거리 측정 알고리즘을 이용한 IP 주소간 거리 분포

을 발송한 서버의 경우 3% 정도만 해당 도메인에 등록된 서버에서 발송되었고, 6% 정도가 비교적 가까운 거리에 존재한다. 이는 스팸메일 발신자의 전자우편 주소가 거의 대부분 조작되었을 가능성이 있음을 암시해 주고 있다.

(그림 6)과 (그림 7)은 각각 클래스 기반 IP 주소간 거리 측정 알고리즘을 이용하여 측정한 IP 주소간 평균 거리와 거리 분포를 보여주고 있다. 이 실험에서는 부-도메인(sub-domain)을 가진 전자우편에 대해서는 상위 도메인을 포함시켜 거리를 측정하였다. 즉, 수신된 전자우편이 subdomain.domain.com이라는 도메인으로부터 왔을 때, 상위 도메인인 domain.com의 DNS 정보도 추가하여 거리를 측정하였다.

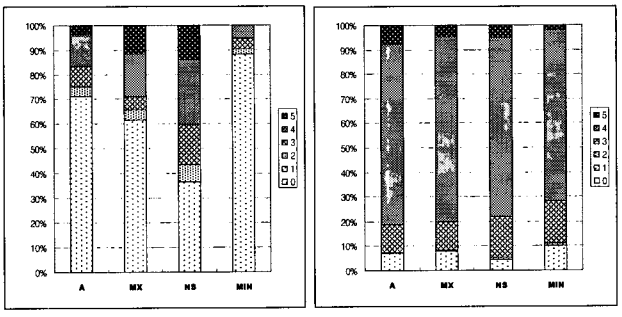
클래스 기반 IP 주소간 거리가 기본 IP 주소간 거리(그림 4와 5 참조)보다 더 확연한 결과를 나타내었다. (그림 6)의 MIN에서 정상메일의 경우 0.436, 스팸메일은 3.421의 평균 거리를 보인다. (그림 4)와 비교했을 때 정상메일의 평균 거리가 더 많이 줄어들었다. 즉, 정상메일과 스팸메일의 평균 거리의 차이가 기본 IP 주소간 거리보다 더 많은 차이가 난다는 것을 알 수 있다.



(그림 6) 클래스 기반 평균 IP 주소간 거리

(그림 7)의 IP 주소간 거리 분포는 (그림 5)와 비교했을 때 거리 3, 4, 5의 비율은 근소하게 줄어 들었다. 그러나 거리 2의 비율은 반으로 줄어들고 거리 1의 비율은 거의 없는 대신에 거리 0의 비율은 줄어든 만큼 늘어났다. 이는 기본 IP 주소간 거리 측정에서 DNS에 등록되어 있지 않았던 일부 전자우편 발송서버들(거리 1 또는 2를 가진 서버들)이 발신자 주소 도메인과 동일한 도메인(또는 지역 네트워크)에 소속된 서버들이라는 것을 의미한다. 그림의 MIN에서 정상메일은 88% 정도가 거리 0을 보이는 반면 스팸메일인 경우 10% 정도가 거리 0을 가진다.

이러한 실험 결과를 통해 스팸메일의 경우 거의 대부분 발신자 전자우편 주소가 조작되었거나 또는 발신자가 소속되지 않은 도메인의 전자우편 발송기를 통해 전자우편을 발송했다는 사실을 확인할 수 있다. 일반적으로 스팸메일 발송기는 도메인에 등록된 서버를 통해 발송하지 않고 개인 PC를 통해 직접 SMTP를 사용하여 대량으로 스팸메일을 발송한다. 2절의 <표 3>과 <표 5>에서 이미 확인했듯이 스팸메일 발송시 발신자의 전자우편 주소를 조작하는데 대부분 전자우편 서비스를 하고 있는 포털 사이트의 도메인을 도용한다.



(a) 정상메일 (b) 스팸메일

(그림 7) 클래스 기반 IP 주소간 거리 분포

이 실험에서 정상메일의 MIN에서는 거리가 5인 전자우편은 없었다. 하지만 거리가 1, 2, 3, 또는 4인 전자우편들이 전체 7,259개 중 864(11.9%)개가 존재하고 있었다. 정상메일임에도 불구하고 거리가 멀리 떨어진 이유를 파악하기 위해 1부터 4사이의 거리를 가지는 정상메일의 전자우편 헤더 정보(Received 필드)와 전자우편의 제목 및 내용 등을 분석하였다.

〈표 6〉 IP 주소 상의 거리가 1,2,3,4인 정상메일들의 분류

분류	개수	%
메일링 리스트	639	74.0
릴레이 된 메일링 리스트	52	6.0
일반 전자우편	72	8.3
릴레이 된 일반 전자우편	101	11.7
합 계	864	100.0

<표 6>은 분석된 전자우편을 종류별로 분류하고 종류별 개수를 보여 준다. 표에서 메일링 리스트란 특정 기관에서 사전에 수신자의 요구 또는 허가에 의해 수집된 전자우편 주소 리스트를 통해 대량으로 발송하는 동일한 내용의 전자우편을 의미하며, 주로 회사 홍보 자료 및 관련 뉴스 등을 포함하고 있다. 이러한 전자우편들을 발송하는 예는 다국적 기업에서 볼 수 있다. 즉, 다국적 기업들은 세계 각국에 지사를 두고 있으며, 각 지사는 해당 전자우편을 자국어로 번역하여 국가별 별도의 전자우편 발송기를 통해 전자우편을 발송하며, 이때 SMTP를 사용하여 발신자의 전자우편 주소를 다국적 기업의 대표 도메인 이름으로 대체한다. 각국의 실제 전자우편 발송기는 별도의 국가별 도메인을 사용하는 경우가 많기 때

문에 다국적 기업의 대표 도메인의 DNS에는 등록이 안될 수 있다. 또한 메일링 리스트는 대량으로 발송되기 때문에 메일링 리스트를 발송하는 서버가 소속되어 있는 네트워크에 혼잡을 발생시킬 수 있다. 따라서 도메인의 네트워크 관리자는 메일링 리스트를 발송하는 서버를 실제 기업의 대표 도메인이 존재하는 네트워크가 아니라, 다른 네트워크로 분리하여 대표 도메인이 존재하는 네트워크의 서비스의 질이 떨어지는 것을 막으려는 의도에서 별도의 전자우편 발송기를 사용하는 경우도 있다.

<표 6>에서 릴레이 된 일반 전자우편이란 발신자가 소속된 도메인과 다른 도메인의 전자우편 발송서버를 통해 전송된 전자우편을 의미한다. 이는 SMTP 설계 시 가능한 가까운 전자우편 발송서버를 통해 전자우편을 발송할 수 있도록 설계되었기 때문이다. 이러한 문제는 현재 표준화가 진행 중인 전자우편 발송서버 권한확인 프로토콜에서도 동일한 문제가 되며, 따라서 IETF의 표준화 단체에서는 가능한 다른 도메인의 전자우편 발송서버의 사용을 지양하도록 권장하고 있다. 따라서 대부분의 도메인에서 전자우편 서버의 릴레이 기능을 차단할 경우 정상메일 중 릴레이 된 전자우편은 점점 줄어들 것으로 판단된다.

<표 6>에서 보인 메일링 리스트 및 일반 전자우편의 특징을 파악하기 위해, 동일한 도메인을 가지는 전자우편들의 개수를 조사하여 <표 7>에 보였다. 표에서 1개의 전자우편만을 전송한 도메인이 77개나 되지만 그 외의 82개의 도메인에서 634개의 전자우편을 전송하였다. 2개 이상의 전자우편을 발송한 도메인에 대해 발송된 전자우편들이 만약 동일한 서버나 또는 동일한 네트워크에 존재하는 서버에서 발송되었다면 사용자의 피드백을 통해 비교적 간단하게 이들을 구제할 수 있다.

〈표 7〉 거리가 1~4인 정상메일의 발송 도메인 통계

동일한 도메인에서 발송한 전자우편 개수	도메인 개수	전자우편 개수의 합계
1	77	77
2	26	52
3	14	42
4	13	52
5	4	20
6 이상	24	468
합계	159	711

따라서 동일한 도메인에 대해 각 전자우편이 발송된 서버의 IP 주소들간의 평균 거리를 측정해 보았다. 즉, 동일한 도메인인 domain.com을 가진 전자우편들이 IP1, IP2 또는 IP3라는 IP 주소를 가진 서버들에 의해 발송되었다면, IP1과 IP2, IP1과 IP3, IP2와 IP3의 클래스 기반 IP 주소간 거리를 계산하여 이들의 평균 거리를 구했다. 그 결과 평균거리의 평균은 0.025, 최소거리는 0, 최대거리는 2의 결과를 얻었다. 0이 아닌 평균 거리는 전체 159개 도메인 중 4개였다. 평균 거리가 2인 도메인은 hanmail.net 이었으며, 총 10통의 전자우편이 세 개의 IP 네트워크 대역을 이용해 발송된 것이었다. hanmail.net은 전자우편을 서비스하는 업체로써 많은 전자우편 전송을 하기 위해 많은 서버를 이용하며, 프리미엄 전자우편 서비스를 제공하여 기본 서비스와의 차등을 제공하기 위해 프리미엄 전자우편 서비스에 대해서는 서버를 따로 둔 것으로 분석되었다. 이 결과는 거리가 1, 2, 3, 4인 정상메일에 대해 한 도메인이 전자우편을 보낼 때에는 동일한 서버 또는 특정한 IP 범위내의 발송서버에서 전자우편을 보낸다는 것을 알 수 있다. 따라서 이러한 정상메일들은 사용자의 피드백을 채택하여 비교적 쉽게 구제할 수 있다.

이상에서 스팸메일로 분류된 정상메일을 피드백을 구제할 수 있음을 보였다. 피드백은 두 가지로 나뉠 수 있다. 먼저 정상메일로 판단된 스팸메일에 대한 피드백이 있다. 이 경우 사용자는 이 전자우편을 제안 방법을 이용하는 스팸메일 차단 엔진에 전달하여 스팸메일임을 알려야 한다. 피드백을 받은 스팸메일 차단 엔진은 피드백에서 어떤 도메인에서 온 전자우편이며, 어떤 IP 주소로부터 왔는가에 대한 통계를 생성한다. 관리자는 이 통계를 기반으로 도메인 및 IP 주소에 대한 블랙리스트를 만들어 새롭게 오는 전자우편에 적용하여 스팸메일을 더 강력하게 차단할 수 있다. 두 번째로 스팸메일로 판단된 정상메일이 있다. 이 전자우편을 구제하기 위해 스팸메일 차단 엔진은 주기적으로 사용자에게 스팸메일 차단 결과를 전송한다. 사용자는 스팸메일 차단 결과를 보고 스팸메일로 판단된 정상메일에 대한 피드백을 스팸메일 차단 엔진에 전송한다. 스팸메일 차단 엔진은 사용자로부터의 피드백을 이용해 정상메일을 구제하며, 정상메일이 발송된 도메인과 IP주소에 대한 통계를 생성한다. 관리자는 이 통계를 기반으로 도메인 및 IP 주소에 대한 화이트리스트를 만들어 새롭게 오는 전자우편에 적용해 정상메일을 더 안전하게 전달할 수 있다.

현재 전자우편 발송서버 권한확인 프로토콜[7, 10, 11, 12]이 표준화 중에 있다. 표준 프로토콜에서는 표준 프로토콜을 사용하지 않는 도메인에서 발송한 전자우편을 차단하지 말고 이전과 같이 받아야 한다고 명시하고 있다. 따라서 표준 프로토콜을 사용하지 않는 도메인에서 발송한 전자우편을 표준 프로토콜을 사용하는 도메인에서 받았을 때, 전자우편을 발송한 서버가 발송 권한을 가지고 있는지 확인하기 위해 본 논문에서 제안한 알고리즘을 사용할 수 있다. 이는 표준 프로토콜이 널리 보편화되어 모든 도메인에서 채택되기 전까지 하나의 보완책으로 활용될 수 있다.

5. 결 론

본 논문에서는 전자우편 발송서버의 권한 확인을 위해 IP 주소간 거리를 활용하는 방안에 대해 논의하였으며, 이를 위해 IP 주소간 거리 측정 알고리즘을 제안했다. 실험을 통해 제안 알고리즘을 활용할 경우 88% 이상의 정상메일을 분류할 수 있음을 보였다. 또한 스팸으로 잘못 분류된 12%의 정상메일도 사용자의 피드백을 이용해 비교적 손쉽게 구제할 수 있음을 확인하였다. 하지만 스팸메일의 차단 비율을 높이고, 정상메일의 차단 비율을 낮추기 위해 사용자의 피드백을 이용하는 것에 대한 구체적인 연구가 필요하다.

제안 알고리즘은 전자우편 발송기를 통해 들어오는 대량의 스팸메일을 효과적으로 차단할 수 있다. 실험 결과에서 확인했듯이 90% 이상의 스팸메일이 발신자 전자우편 주소의 도메인 부분을 조작하고 있기 때문에 IP 주소간 거리가 상대적으로 크다. 따라서 본 논문에서 제안하는 IP 주소간 거리를 이용하여 다수의 스팸메일을 차단할 수 있으며, 전자우편 발송서버 권한확인 표준 프로토콜을 사용하지 않는 도메인에 대해서 전자우편 발송서버의 권한을 확인하는데 활용할 수 있다.

스팸메일의 경우 다양한 네트워크에서 전자우편을 발송하고 있으며, 정상메일의 경우 제한된 네트워크에서 전자우편을 발송하고 있다. 따라서 정상메일을 발송하는 네트워크를 점진적으로 찾아가는 알고리즘을 통해 DNS로의 접속 회수를 줄일 경우 제안 알고리즘을 보다 효율적으로 수행할 수 있다.

참 고 문 헌

[1] "Why is spam bad?" http://spam.abuse.net/overview/spambad.shtml

[2] S. Hird, "Technical Solution for Controlling Spam," *Proc. of AUUG (The Australian Unix systems User Group)*, Melbourne, Sept., 2002.

[3] L. F. Cranor and B. A. LaMacchia, "Spam!", *Communications of the ACM*, Vol.41, No.8, pp.74-83, Aug., 1998.

[4] G. Sakkis, I. Androutsopoulos, G. Paliouras, V. Karkaletsis, C. Spyropoulos, and P. Stamatopoulos, "A Memory-Based Approach to Anti-Spam Filtering," *Tech. Report DEMO*, National Centre for Scientific Research (NCSR) : Demokritos, Athens, 2001.

[5] I. Androutsopoulos, J. Koutsias, K. V. Chandrinos, G. Paliouras, and C. D. Spyropoulos, "An Evaluation of Naive Bayesian Anti-Spam Filtering," *Proc. of the Workshop on Machine Learning in the New Information Age*, 2000.

[6] B. Templeton, "Proper Principles for Challenge/Response Anti-Spam Systems," http://www.templetons.com/brad/spam/challengeresponse.html

[7] H. Danisch, "The RMX DNS RR and Method for Lightweight SMTP Sender Authorization," Oct. 2003, http://www.danisch.de/work/security/txt/draft-danisch-dns-rr-smtp-03.txt

[8] "전자우편 주소 추출 방지 S/W : NeverSpam", http://www.spamcop.or.kr/swDown/pg_email.jsp

[9] E. Gabber, M. Jakobsson. Y. Matias, and A. J. Mayer, "Curbing Junk E-mail via Secure Classification," *Proc. of the Second International Conference on Financial Cryptography*, pp.198-213, Feb., 1998.

[10] Microsoft Corporation, "Caller ID for E-mail : The Next Step to Deterring Spam," Feb., 2004.

[11] M. W. Wong and M. Lentczner. "Sender Policy Frame work(SPF) : A Convention to Describe Hosts Authorized to Send SMTP Traffic," May 2004, http://www.danisch.de/work/security/txt/draft-mengwong-spf-01.txt

[12] H. Danisch, "SCAF - Simple Caller Authorization Framework," Jan. 2004, http://www.danisch.de/work/security/txt/draft-danisch-scaf-00.txt

[13] G. S. Malkin, "RFC2453 - RIP Version 2," Nov., 1998.

임 호 성

e-mail : hsyim@dinnovan.com

2003년 아주대학교 정보및컴퓨터공학부(학사)

2005년 아주대학교 정보통신전문대학원 정보통신공학과(석사)

2005년~현재 디노밴㈜ 정보통신연구소 연구원

관심분야 : 운영체제, 인터넷 표준 규약, VoIP

심 재 홍

e-mail : jhshim@chosun.ac.kr

1987년 서울대학교 전산과학과(학사)

1989년 아주대학교 컴퓨터공학과(석사)

2001년 아주대학교 컴퓨터공학과(박사)

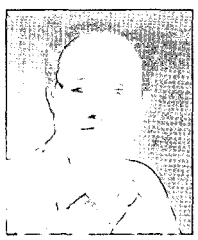
1989년~1994년 서울시스템(주) 공학연구소

1999년~2000년 University of Arizona 객원연구원

2001년~2001년 아주대학교 정보통신전문대학원 BK21 전임연구원

2001년~현재 조선대학교 인터넷소프트웨어공학부 조교수

관심분야 : 임베디드시스템, 운영 체제, 분산시스템, 실시간 및 멀티미디어시스템



최 경 희

e-mail : khchoi@madang.ajou.ac.kr

1976년 서울대학교 수학교육과(학사)

1979년 프랑스 그랑제꼴 Enseeiht대학(석사)

1982년 프랑스 Paul Sabatier대학 정보공학부(박사)

1982년~현재 아주대학교 정보통신전문대학원 교수

관심분야 : 운영 체제, 분산시스템, 실시간 및 멀티미디어시스템 등

정 기 현

e-mail : khchung@madang.ajou.ac.kr

1984년 서강대학교 전자공학과(학사)

1988년 미국 Ilinois주립대 EECS(석사)

1990년 미국 Purdue대학 전기전자공학부(박사)

1991년~1992년 현대반도체 연구소

1993년~현재 아주대학교 전자공학부 교수

관심분야 : 컴퓨터구조, VLSI 설계, 멀티미디어 및 실시간 시스템 등