한국시뮬레이션학회 논문지
Vol. 16, No. 3, pp. 75-87 (2007. 9)

VoIP 스팸 콜 탐지를 위한 음성신호의 DEVS 모델링 및 시뮬레이션

김지연[1] · 김형종[1†] · 조영덕[2] · 김환국[2] · 원유재[2] · 김명주[1]

DEVS Simulation of Spam Voice Signal Detection in VoIP Service

Ji-Yeon Kim · Hyung-Jong Kim · Young-Duk Cho · Hwan-Kuk Kim · Yoo-Jae Won · Myuhng-Joo Kim

ABSTRACT

As the VoIP service quality is getting better and many shortcomings are being overcome, users are getting interested in this service. Also, there are several additional features that provide a convenience to users such as presence service, instant messaging service and so on. But, as there are always two sides of coin, some security issues have users hesitate to make use of it. This paper deals with one of the issues, the VoIP spam problem. We took into account the signal pattern of voice message in spam call and we have constructed voice signal models of normal call, normal call with noise and spam call. Each voice signal case is inserted into our spam decision algorithm which detects the spam calls based on the amount of information in the call signal. We made use of the DEVS-Java™ for our modeling and simulation. The contribution of this work is in suggestion of a way to detect voice spam call signal and testing of the method using modeling and simulation methodology.

Key words : VoIP spam, Greylist, Discrete event simulation, DEVS formalism

요 약

VoIP 서비스 품질이 개선되고 많은 문제점들이 극복되면서 이에 대한 사용자들의 관심이 높아지고 있다. VoIP는 인스턴트 메시징 서비스 등 사용자들의 편익을 위한 서비스를 제공하고 있지만 비용 및 보안 문제는 사용자들의 이러한 서비스 사용을 주저하게 만들고 있다. 본 논문은 이와 같은 문제 중 하나인 VoIP 스팸 문제를 다루고자 한다. 스팸 콜에서의 음성 메시지 신호 패턴을 고려하여 정상 콜과 Noise가 포함된 정상 콜, 스팸 콜 이 세 가지 음성 모델을 설계하고, 논문에서 제시하는 음성 신호 정보량 기반의 스팸 탐지 알고리즘에 적용해 보았다. 각 모델의 모델링 및 시뮬레이션은 DEVS-Java™를 이용하였다. 본 연구는 스팸 콜 음성 신호를 탐지하기 위한 방법을 제시하고 이를 모델링 및 시뮬레이션 방법론을 통해 검증하는 것에 기여점을 둘 수 있다.

주요어 : VoIP 스팸, 그레이리스트, 이산사건 시뮬레이션, DEVS 형식론

1. 서 론

VoIP(Voice over Internet Protocol)는 IP(Internet Protocol) 기반으로 운영되는 네트워크를 통해 음성 대화(Voice Conversation)를 라우팅하는 것을 말한다. VoIP 기술은 음성 통신에 사용되던 PSTN망을 IP망으로 대체하기 위한 기술로서 IP망이 갖는 유휴 자원을 활용하는 차원에서 저렴한 비용의 전화서비스를 제공하면서 초기 시장을 점유하였지만, 기존 PSTN 망을 통해 비교적 안정적인 서비스를 제공받던 사용자들에게는 불안한 연결설정 및 낮은 통화품질로 외면당하였다. 그러나 최근 IP 네트워크에 대한 안정적 관리가 이루어지고 각 가정에 광대역 인터넷 망(100Mbps 급)이 보급 되면서, IP 망을 사용한 음성 통신에 대한 관심이 고조되고 있다. 인터넷 및 전화서비스 사업자들은 IP기반 교환기를 적극적으로 도입하고 있으며 최근에는 한번에 1000명의 통화를 처리할

* 본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음[2006-S-043-02, VoIP정보보호기술]
2007년 9월 10일 접수, 2007년 9월 20일 채택
[1] 서울여자대학교 컴퓨터학부
[2] 한국정보보호진흥원
주 저 자 : 김지연
교신저자 : 김형종
E-mail; hkim@swu.ac.kr

수 있는 교환기가 도입되어 사용되고 있다. 이러한 서비스 제공자들의 행보는 VoIP 기반의 전화 서비스가 갖는 가격 경쟁력과 화상 통화를 비롯한 각종 부가 서비스가 갖는 장점에 대해 기업 및 가정에서 매력을 느끼는데서 비롯된 것이다. 그러나 VoIP의 대표적 특징인 개방된 네트워크(TCP/IP 기반 인터넷)를 통해 서비스가 제공된다는 점은 IP망이 기본적으로 내포하고 있는 보안 문제 및 이와 연관된 스팸 문제를 유발시켰고, 2005년도 VOIPSA (Voice Over IP Security Association)에서 발간된 위협 분류(Threat Taxonomy)에서는 VoIP 스팸을 원하지 않는 합법적 콘텐츠(Unwanted Lawful Contents)로 분류하였다. VoIP 스팸은 기존의 이메일이나 휴대폰, 전화 기반의 통신 서비스에 비하여 훨씬 더 복잡하고 대량적일 것으로 예상되어 그 심각성이 매우 크고, 이 때문에 현재 관리자 및 사용자에게 있어 스팸이 가장 큰 문제가 되고 있는 이메일 서비스는 VoIP에게 시사 하는바가 크다고 할 수 있다. 스팸 메일은 메일 수신자 관점에서는 원치 않는 메일 수신으로 인한 쓸모없는 메일 확인 및 삭제 등의 시간 낭비를 가져오고, 시스템 혹은 네트워크 관리자 입장에서는 조직의 목적과 관련 없는 트래픽으로 인한 대역폭의 낭비와 과도한 메일 수신으로 인한 메일 서버의 컴퓨팅 자원 낭비를 가져온다.

이러한 스팸메일에 대한 피해를 최소화하기 위한 필터링 기법에는 메일에 포함된 단어의 통계치를 이용한 베이지안 필터링, 메일 근원지 정보의 진실성을 검증하기 위한 SPF(Send Policy Framework), RBL(Real Block List), 메일의 특정 정보를 기반으로 전자서명 기법을 사용하고 수신자로 하여금 공개키를 사용한 복호화를 통해 이를 검증하게 하는 도메인 키 기법, 자동화된 메일 송수신 정보의 관리를 통해 스팸발송자를 분류하는 그레이리스트 등이 사용되고 있고, 이들 기법 중에 베이지안 필터링을 제외한 모든 기법들은 VoIP 스팸 필터링에도 적용이 가능할 것으로 본다. 다만 VoIP는 사용자와 프록시 서버가 SIP에 의해 움직이므로 이메일의 그레이리스트처럼 임시 오류를 통한 스팸 필터링은 기대할 수 없다. 따라서 본 논문에서의 그레이리스트는 이메일의 경우처럼 일시적으로 거부된 화이트리스트의 개념이 아니라, 화이트리스트인지 블랙리스트인지 아직 구분이 되지 않는 VoIP 콜에 대한 리스트로 정의하기로 한다.

본 논문은 위에 소개된 스팸 필터링 기법들 중 그레이리스트에 기반 하여 VoIP 스팸 콜을 탐지하는 알고리즘을 제안하고 이를 DEVS 형식론을 적용하여 모델을 구성한다. 그리고 콜의 속성에 따라 세 가지의 음성 모델을 설계하고 이를 제시된 알고리즘에 적용하여 시뮬레이션을 수행함으로써 모델의 효율성과 능력을 검증하고자 한다.

논문의 구성은 2장에서 본 연구의 배경이 되는 스팸메일 필터링 기법과 DEVS 형식론을 소개하고 3장에서 VoIP 스팸 탐지 모델링을 통해 스팸 콜 탐지 알고리즘을 제시한다. 4장에서는 콜 속성별 시뮬레이션 결과를 분석함으로써 모델을 검증하고 5장에서 결론 및 향후 연구계획을 제시하도록 한다.

2. 관련 연구

2.1 DEVS 형식론

DEVS[9]는 계층적이고 모듈화 된 이산 사건 시스템을 표현하기 위한 방법론으로서 집합이론을 기반으로 체계적으로 정립된 형식론이다. DEVS에서 대상 시스템은 시간을 기반으로 하는 입력, 상태, 출력, 상태 변환 함수들로 표현되며, 함수들은 현재 상태와 입력을 근거로 하여 다음 상태와 출력을 결정하게 된다. DEVS 형식론에서 시스템을 기술하기 위한 두 가지 모델 유형, 기본(basic) 모델과 결합(coupled) 모델이 있다. 기본 모델(M)은 시스템의 동작(behavior)의 단위가 되는 시스템의 구성 요소들을 표현하기 위한 것이고, 결합 모델(DN)은 시스템의 구성 요소 간의 상호작용을 의미하는 구조(structure)를 표현하기 위한 것이다. 다음은 이 두 모델의 구성 요소이다. 기본모델 $M = < X, S, Y, \delta_{int}, \delta_{ext}, \lambda, ta >$이며 이 때 X, S, Y는 각각 입력 이벤트, 상태, 출력 이벤트의 집합이고, δ_{int}, δ_{ext}는 각각 내부 상태 변이, 외부 상태 변이 함수이며 λ와 ta는 출력 및 시간 갱신 함수이다. 결합모델 $DN = < D, \{M_i\}, \{I_i\}, \{Z_{ij}\}, select>$ 이며, 이 때 D는 구성 요소가 되는 모델들의 이름 집합을, M_i 은 구성 요소가 되는 I번째 모델을, I_i 는 모델 I가 영향 주는 다른 모델들의 집합을 의미하고 Z_{ij} 는 모델 I에서 모델 j로의 연결 함수를 의미한다[8].

2.2 스팸 메일 필터링 기술

기술된 전자메일의 스팸 필터링 기법은 스팸 메일에 대응하기 위한 대표적인 기술로서 메일 서버 측면에서 활용되고, 이의 결과가 메일 클라이언트에 도착할 때 사용자가 지정한 간단한 규칙을 통해 추가적인 필터링이 가능하게 된다.

2.2.1 베이지안 필터링

콘텐츠 필터링인 베이지안(Bayesian) 필터링은 다수개

의 독립적인 사건으로 인해 발생할 특정 사건의 확률을 하나의 확률변수에 지정하는 방법이다. 식(1)은 단순화된 베이지안 필터링 기법이다.

$$P(E_j|F) = \frac{P(F|E_j)P(E_j)}{\sum P(F|E_i)P(E_i)} \quad (1)$$

베이지안 필터링 기술은 이메일 내용의 특정 단어 발생에 적용하여 추가적인 스팸관련 단어가 발생할 경우 이를 반영하여 스팸 추정 단어 집합인 스팸 패턴을 만들고, 이렇게 만들어진 스팸 패턴을 기준으로 스팸 메일을 필터링한다. 베이지안 필터링의 장점은 확률변수에 근거하여 수학적 모델에 기반 한다는 것이고 이것은 관리자의 개입과 직관적 판단을 배제하여 신뢰성을 높여준다. 또 주기적으로 스팸 패턴을 업데이트함으로써 스팸의 성격이 달라지는 것에 대한 빠른 대응이 가능하다. 이처럼 베이지안 필터링이 이메일에 대한 콘텐츠 필터링으로서는 1차 혹은 복합적인 필터링으로 스팸 차단의 성능이 뛰어나지만 스팸 콜이 발생했을 때 전화를 받기 전까지는 송신자의 의도와 전달할 콘텐츠의 내용을 알 수 없고[1,13], 음성을 토큰 단위로 정확히 나누어 필터링 한다는 것이 실제적 필터링 기술적용에 있어 어려움이 있으므로 VoIP 스팸 콜에 대한 필터링으로 사용하기에는 부적절하다.

2.2.2 SPF(Sender Policy Framework)

SPF는 이메일 송신자의 발송 서버 도메인과 IP 주소를 매핑 시켜 특정 도메인의 메일은 특정 IP에서만 전송되도록 정하는 것이다. 사용자가 이메일 주소를 스푸핑(Spoofing)하여 스팸 메일을 보내는 경우 그것을 탐지하는 목적으로 사용 할 수 있다. 송신자는 사전에 SPF 정보인 도메인과 IP주소를 DNS 서버에 전송하여 SPF 레코드에 등록 및 저장을 하고, 수신자는 DNS 서버에 송신자의 IP주소를 사용하여 질의를 보낸 후 송신 IP가 SPF 정책에 맞는 이메일임을 확인하면 수신자의 메일함에 보내준다[3]. 그림 1은 SPF의 송신자 및 수신자가 각각 수행하는 과정을 나타낸 것이다.

SPF를 VoIP 스팸 차단에 활용하기 위해서는 VoIP를 위한 별도의 SPF 서버가 필요하다. 발신측 SIP 프록시 서버 및 소프트스위치의 IP 주소와 해당 IP 주소에 연결되어 있는 도메인 정보를 SPF 서버에 저장관리하고, 수신측 SIP 프록시 서버에서는 SPF 서버에 질의를 통하여 해당 IP 및 ID 정보에 대한 등록여부를 확인하여 등록되어 있지 않을 경우 VoIP 콜을 차단한다.

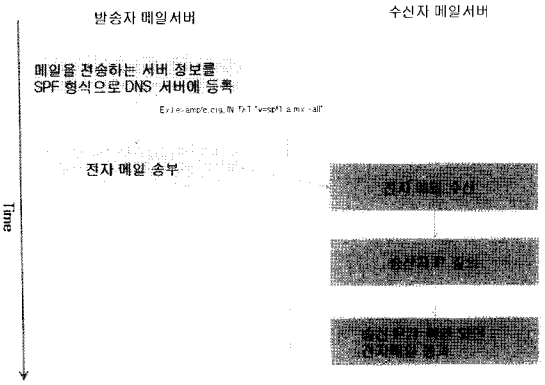


그림 1. SPF의 수행 과정

2.2.3 RBL(Real Time Block List)

RBL 시스템은 차단 신고 된 IP정보를 실시간으로 참조하여 해당 IP에서 온 메일을 수신자의 메일함에 넣을 것인지 아닌지를 결정하는 동작을 한다. RBL을 활용하여 스팸을 필터링하는 경우에는 RBL IP 정보를 제공해주는 서버가 존재해야 한다. 이러한 서버 역할을 해주는 시스템에 DNS 룩업(lookup) 형태의 요청을 통해 해당 IP가 블랙리스트에 들어 있는 IP인지 아닌지를 파악할 수 있다. 일반 메일 서버에서 RBL 룩업을 하게 되면 DNS 질의를 과도하게 할 수 밖에 없는데, RBL 룩업의 경우에는 대부분의 질의가 failure로 끝나는 것이 정상적인 경우이므로 DNS 서버에 과도한 부하를 일으키게 된다. 이 때문에 일반적으로는 DNS 서버를 사용하지 않고 스팸메일 차단 전용으로 RBL DNS 데몬을 별도로 메일 서버에 설치해서 사용한다. 사전에 DNS 서버에 저장되어 있는 SPF 형식의 데이터는 DNS 질의를 통해 수신측에서 조회가 가능하고, 이러한 조회를 통해서 정상적인 IP로 확인이 되면 해당 이메일은 사용자에게 전달된다.

RBL은 개념적으로 매우 간단한 정책이므로 VoIP 서비스에 적용하는 데에 어려움은 없지만 RBL을 조성하기 위한 근원 데이터를 입수하는 방식이 이메일보다 복잡해질 수 있다. VoIP용 RBL을 형성하는 데에 있어서 이메일과 동일한 근원 데이터 입수 방식은 사용자의 신고이다. VoIP 스팸을 수신한 사용자는 자신의 단말기에도 블랙리스트로 해당 발신자를 등록할 뿐만 아니라, 간편 신고 제도를 통하여 수신측 프록시 서버로 보내게 된다. 수신 프록시 서버는 간편 신고를 통하여 접수한 새로운 블랙리스트 IP 주소를 중앙관리기구(KISA)에 단순히 전달만 해줄 수도 있고, 자신이 어느 정도 종합판단절차를 취하여 나름대로의 RBL(이것을 Local RBL이라고 부름)을 형성하

여 자체에서 적용할 수도 있으며 이 Local RBL을 주기적으로 중앙 관리 기구에 전송하여 Global RBL을 생성하는 데에 일조할 수도 있다. 어느 방법을 사용하는 것이 좋은지는 RBL 도입에 따른 효율성과 관련이 있고, 이메일 스팸용 RBL에서 나타나는 DNS 서버 집중현상이 프록시 서버나 중앙관리서버에도 나타날 수 있으므로 이들에 대한 집중현상을 감안하여 정책을 채택하는 것이 좋을 것이다.

2.2.4 그레이리스팅(Greylisting)

그레이리스트(Greylist) 기법은 기존의 블랙리스트 혹은 화이트리스트 기법이 갖는 이분법적인 분류를 지양하고 자동화된 메일 수신, 송신 정보의 관리를 통해 스팸발송자를 분류해 내는 기술이다. 대부분의 스팸 메일 발송자들이 "fire and forget"형태로 스팸을 보내는 특성 즉, 어떤 메일을 받았을 때 만일 해당 메일의 관리정보가 처음 송신된 경우 이에 대해 "일시적 실패"(Temporary failure)로 응답을 보내주고, 스팸발송자는 정상 메일서버들이 사용하는 발송대기 큐를 활용하여 일정 시간 후 다시 보내주거나 스팸메일의 전송을 포기하게 된다. 이러한 그레이리스트 메커니즘은 자동 스팸메일 발송도구 대부분의 메일 송신을 차단할 뿐만 아니라, 웜 바이러스에 의해 전송되는 스팸에도 매우 효과적인 것으로 알려지고 있다. 또한 발송자의 IP주소와 메일 주소, 수신자의 메일 주소만을 저장하기 때문에 수신 서버의 자원을 최소화 할 수 있고, 본문 모두를 분석해야하는 콘텐츠 필터링에 비해 트래픽을 줄이고 수신 서버의 부하를 막을 수 있어 절약효과가 크다. 그레이리스트는 메일 발송 시 임시 에러 전송으로 인해 지연이 되는데 이것은 스패머에게 많은 부담을 가중케 해 스팸 차단 지수를 높인다.

2.2.5 도메인 키(Domain Key)

송신자 서명 정책(Sender Signing Policy)이라고도 하는 도메인 키 기법은 메일을 발송하는 사람이 발송 시점에 메일의 "송신자정보", "수신자정보", "발송시점" "제목" "내용"에 대해 전자서명을 수행하여 서명된 해시 값(도메인 서명)을 헤더에 붙여 보내고, 메일 수신자는 DNS로부터 받은 공개키를 활용하여 서명된 해시 값을 복호화하여 메일을 검증한다. 그림 2는 이러한 도메인 키의 메일 전달 절차를 보여 주고 있다. 도메인 키를 사용한 메일발송은 스팸메일이 갖는 근원지에 대한 불확실성을 거의 완전히 해결해 준 솔루션이라고 할 수 있지만, 메일 전송 시 마다 서명을 수행하고 메일 수신 시 마다 복호화를 통해 검증함으로써 갖는 오버헤드를 단점으로 지적 할 수 있다.

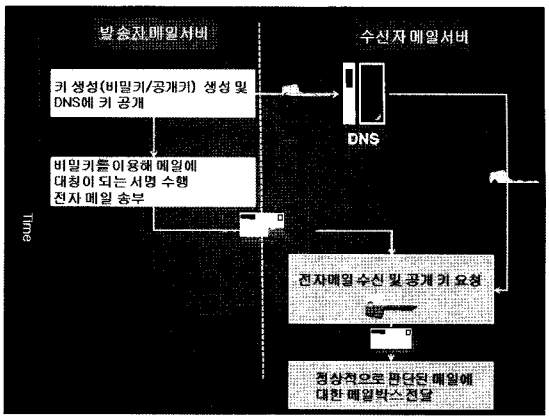


그림 2. 도메인 키 기법의 메일 전달 절차

도메인 키를 사용하는 VoIP 서비스의 경우, 스팸 콜의 발신자에 대한 불확실성을 거의 제거해준다는 점에서는 희망적인 기법이지만 정상 발신자의 경우에도 매번 서명을 수행한다는 점이나 반대로 콜 수신시에도 역시 복호화를 통한 검증이 필요하다는 점으로 인한 오버헤드가 현실적인 어려움으로 대두된다. 특히 사전에 VoIP 고객용 공개키가 모두 DNS에 등록되어 보급되어야 하고, VoIP가 단독 운영이 아닌 기존의 유무선 전화와 연동될 수 있다는 점에서 도메인 키 기법을 적용하려면 현실적인 문제들을 풀어야 할 것이다.

3. VoIP 콜 스팸 탐지 모델

3.1 VoIP 콜 스팸 탐지 알고리즘

그레이리스트에 기반한 VoIP 콜 스팸 탐지는 적용 알고리즘에 따른 콜 패턴의 통계적 특성에 의해 이루어진다. 콜 흐름의 패턴 분석을 위해서는 음성 신호의 부호화 작업이 필요하고, 현재 대부분의 VoIP 망에서는 ITU의 G.729a 코덱을 사용하고 있다[15]. G.729a는 음성신호를 프레임 단위마다 '합성에 의한 분석(Analysis by Synthesis)을 이용한 선형예측 방법'으로 부호화하는 코덱으로서, 프레임 길이는 10ms, 음성은 8Kbps로 압축한다[16,17]. 이에 본 논문은 G.729a를 기반으로 콜 흐름의 패턴을 분석함으로써 VoIP 콜 스팸을 탐지하는 알고리즘을 제시하고자 한다.

먼저 분석 단위 구간(n)을 설정하고 이 구간의 음성 메시지의 양($q(t)$)에 기반 하여 평균이 임계값(*Mean_Threshold*) 이상이면 의미 있는 메시지(meaningful message) 전송 구간, 임계값 미만이면 의미 없는 메시지(meaningless

message) 전송 구간이라고 정의한다. 그리고 그림 3에서 t_0~t_n은 *Mean_Threshold* 미만의 메시지를, t_n~t_{2n}은 *Mean_Threshold* 이상의 메시지를 전송하였다고 가정한다면, t_0~t_n은 meaningless message 전송 구간, t_n~t_{2n}은 meaningful message 전송 구간으로 볼 수 있다.

if $(\frac{1}{n}\int_{t_0}^{t_n} q(t)dt \leq Mean\_Threshold)$

Then No-Meaning during that time period(t_0~t_n)

Else There is meaning in the traffic during that time period(t_0~t_n)

$q(t)$: Quantity of Message in a given time slot

$Mean\_Threshold$:

Threshold for determining whether meaningful or meaningless

일반적으로 스팸이 아닌 정상 콜의 경우에는 대화를 주고받는 사이에 대화가 멈추는 시간이 존재하므로 meaningful message 전송 구간과 meaningless message 전송 구간이 반복될 것이다. 하지만 ARS와 같은 스팸성 콘텐츠가 전달되고 있다면 meaningful message가 거의 쉼 없이(without pause) 전달될 것이고 이러한 경우에는 스팸 콜로 분류 할 수 있다.

3.2 VoIP 콜 스팸 탐지 시뮬레이션 설계

VoIP 콜 스팸 탐지 시뮬레이션을 위한 모델은 그림 4와 같이 Proxy Server, Caller, Callee로 구성된다.

Proxy Server모델은 Caller와 Callee의 매개체로 각 모델을 대신하여 요청을 전달해주고, Caller는 VoIP의 송신자로서 콜을 생성하는 모델이다.

Callee 모델은 VoIP 콜을 수신하는 모델이고 앞에서 제시한 스팸 탐지 알고리즘에 기반 하여 스팸 여부를 결정하는 Greylist management Algorithm 모델을 포함한다.

G.729a 코덱과 같이 10ms 간격으로 8bit로 압축된 음성 신호를 샘플링하면 그 신호는 0~255의 값을 나타낼 수 있다. 이를 기반으로 의미 없는 메시지는 0~127, 의미 있는 메시지는 128~255의 값을 가지고 있다고 가정한다면 여기서의 *Mean_Threshold* 값은 128로 설정할 수 있다. 또한, t_0~t_n, t_1~t_{n+1}, ……, t_i~t_{n+i} 각 분석 구간의 평균 $q(t)$에 대하여 어떠한 구간도 *Mean_Threshold* 미만의 값을 가지고 있지 않다면, 이 콜은 meaningful message만 쉼 없이 전달된 것으로 간주하여 스팸 콜로 판단할 수 있을 것이다.

그림 5는 Callee 모델의 구성을 보여주고, 표 1은 이와 같은 Greylist Management Algorithm 모델의 의사코드를 나타낸다.

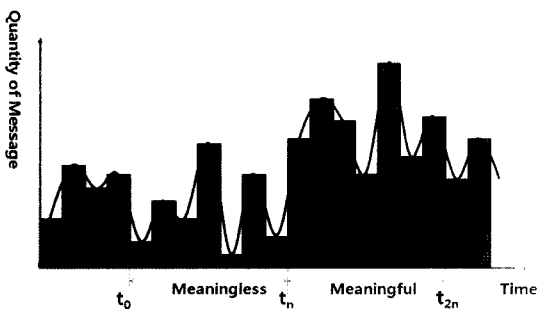


그림 3. 음성 메시지 Meaning abstraction

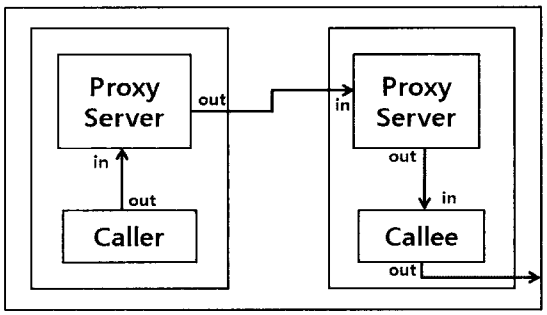


그림 4. VoIP 콜 스팸 탐지 시뮬레이션

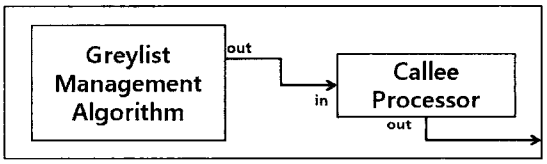


그림 5. Callee 모델

표 1. Greylist Management Algorithm 모델 의사코드

External Transition

```
if receive the message on port 'in_val'
   if (t_i~t_n+i)average of q(t)  <  Mean_Threshold
            non-Spam Call
   else
            Spam  Call

if receive the message on port 'in'
   if message is not "Bye"
            Hold-in 'busy'
   else
            Hold-in 'bye'
```

```
Internal Transition
if phase is 'busy'
    if buffer is not empty
            Keep the state

else
    Hold-in 'passive'

Output
if phase is 'bye'
    if result is Spam call
            send message "SPAM"
                    on port 'out_value'
    else
            send message "NON-SPAM"
                    on port     'out_value'
    send message "Bye" on port 'out'

else
    send the message on port 'out' and out_value'
```

4. 실험 및 결과 분석

4.1 시뮬레이션 방법

VoIP 스팸 콜 탐지 모델을 보다 정확하게 검증하기 위해서는 다양한 속성의 콜에 대하여 시뮬레이션을 수행 할 필요가 있다. 이것은 콜의 외적 환경 또는 검증 방법, 알고리즘의 동적 속성으로 인해 스팸 콜이 정상 콜로 결정되거나 반대로 정상 콜이 스팸 콜로 결정되는 등의 많은 예외상황이 발생하기 때문이다. 따라서 본 논문에서는 콜 속성에 따라 세 가지 음성 모델을 제시하고 이 세 가지 모델에 대하여 음성 신호를 발생시켜 시뮬레이션을 수행하도록 하였다.

첫 번째는 모델은 정상 콜(Non-Spam Call)이다. 이 모델은 외부 환경이 콜에 영향을 미치지 않고 콜의 형태도 송신자와 수신자가 대화를 주고받는 정상 콜의 형태를 보인다. 이러한 콜은 대화를 주고받는 사이에 대화가 중단되는 구간이 많이 발생하게 되고, 일반적으로 이 구간의 합은 전체의 약 35%에 해당된다. 시뮬레이션에서는 이 구간을 meaningless message 전송 구간으로 정의하였고, 이 수치를 기반으로 하여 콜의 음성 신호를 발생시키도록 하였다. 두 번째는 모델은 Noise가 포함된 정상 콜(Noise Call)로서 첫 번째 모델과 같이 송수신자 간에 정상적인 콜 형태의 대화를 주고받는다. 하지만 콜 배경에 일정한 Noise가 존재한다는 가정 하에 이 값을 적용하여 콜의 음성 신호를 발생시킨다. 세 번째 모델은 일반적인 스팸 콜(Spam Call)의 형태이며 스팸 콘텐츠가 수신자에게 전달된다. 스팸 콘텐츠가 전송되는 경우에는 대화를 주고받을 때처럼 많은 meaningless message 전송 구간이 발생하지는 않지만 콘텐츠 상에 존재하는 몇몇의 짧은 meaningless message 전송 구간이 존재하게 된다. 일반적으로 스팸 콘텐츠의 meaningless message 전송 구간은 전체 콜의 약 10%에 해당되고, 이 수치를 적용하여 세 번째 콜 모델의 음성 신호를 발생시키도록 하였다.

위의 세 가지 모델에 대하여 콜의 길이는 모두 30초, meaningful message는 128~255 값으로 생성되도록 설정하였다. 다만 meaningful message 전송 구간이 길게 존재 하는 Spam Call 모델의 경우에는 이 구간을 8초~9.5초로 길게 발생 시키고 Non-Spam Call 모델과 Noise Call 모델에서는 4초~5.5초로 발생시키도록 하였다. 반대로 meaningless message 전송 구간에 대해서는 Spam Call 모델은 1초~2.5초로 짧게 발생시키고 나머지 두 모델에서는 상대적으로 길게 2초~3.5초의 값을 생성하도록 하였다. meaningless message는 0~127 값을 갖도록 하였는데 Noise Call 모델에서는 Noise가 64의 값을 가지고 있다고 가정하였기 때문에 이 값을 반영한 64~191 값을 생성하도록 한다.

위에서 제시한 세 가지 시뮬레이션 모델에 대한 음성 신호의 발생 값은 그림 6과 같다.

4.2 시뮬레이션 결과

시뮬레이션 결과에 영향을 미치는 요소로는 입력된 음성 신호, 콜의 스팸 판단의 기준이 되는 *Mean_Threshold*, 음성신호의 분석 단위 시간 이렇게 세 가지가 있다. 입력 음성 신호에 대해서는 앞에서 세 가지 모델을 제시하였는데, 각각의 모델별로 음성신호를 발생시키는 랜덤함수의 seed값을 5번씩 변경하여 총 15가지의 입력에 대한 시뮬레이션을 수행하도록 한다. *Mean_Threshold*는 128로 고정하여 분석 구간의 음성 신호 평균이 128 이상이면 스팸, 미만이면 스팸이 아닌 콜로 결정하기로 한다. 분석 단위 시간은 세 가지 모델의 meaningless message, meaningful message 전송 구간을 포함할 수 있는 1500ms, 3500ms, 5500ms로 설정하고 각 시간을 기준으로 시뮬레이션을 수행했을 때 콜의 스팸여부가 어떻게 달라지는지 살펴보도록 하겠다.

시뮬레이션 결과 그림은 Non-Spam Call 모델, Noise Call 모델, Spam Call 모델별로 seed 값을 1, 2, 3, 4, 5로 설정한 5가지 그림이 있으며, 하나의 그림은 세 경우의 분석 단위 시간 1500ms, 3500ms, 5500ms의 그래프를 함께 보여준다. y축은 분석 단위 구간의 음성 신호 평균을 나타내고 이 값이 *Mean_Threshold* 즉, 128 미만인 경

우가 한번이라도 존재한다면 제시된 알고리즘에 의해 스팸이 아닌 콜로 판단 할 수 있다.

그림 7은 Non-Spam Call 모델의 결과를 보여준다.

Non-Spam Call 모델의 경우에는 5개의 seed값에 대하여 분석 단위 시간이 1500ms, 3500ms, 5500ms인 경우모두 음성 신호 평균이 1번 이상 128미만 값이 존재하므로 15가지 경우가 Non-Spam Call로 결정되었음을 알 수 있다. 이것은 Non-Spam Call 모델이 변수를 일으킬만한 외적 요소를 하나도 갖고 있지 않고 검증 방법도 적절했기 때문에 나타나는 결과로 생각할 수 있다. 따라서 이 모델을 알고리즘의 정상 콜을 탐지하는 기본 모델로 설정할 수 있을 것이다. 그림 8은 Noise Call 모델의 결과 그래프이다.

Noise Call 모델의 시뮬레이션 결과를 살펴보면 1500ms로 분석 단위 시간을 설정했을 때에는 5가지 seed값에 대하여 모두 Non-Spam으로 결정되었는데 이것은 1500ms라는 시간이 Non-Spam Call 모델의 meaningless message 전송 구간 보다 작은 경우이기 때문에 나온 당연한 결과이다. 3500ms인 경우는 seed값이 3, 5인 경우에 Non-Spam으로 결정되었으나 Non-Spam으로 나온 구간의 평균도 모두 127이상인 것을 보면 거의 Spam에 가깝다고 생각할 수 있다. 5500ms로 분석 단위 시간을 길게 하였을 경우에는 모두 Spam으로 결정되었다. 이와 같이 Noise 값이 Non-Spam Call을 Spam Call로 인식하도록 시뮬레이션 결과에 영향을 미치는 것을 볼 때, 스팸 콜을 탐지하는데 있어서 Noise는 고려되어야 할 매우 중요한 외부 요소로 생각할 수 있다.

그림 9는 Spam Call 모델의 결과 그래프이다.

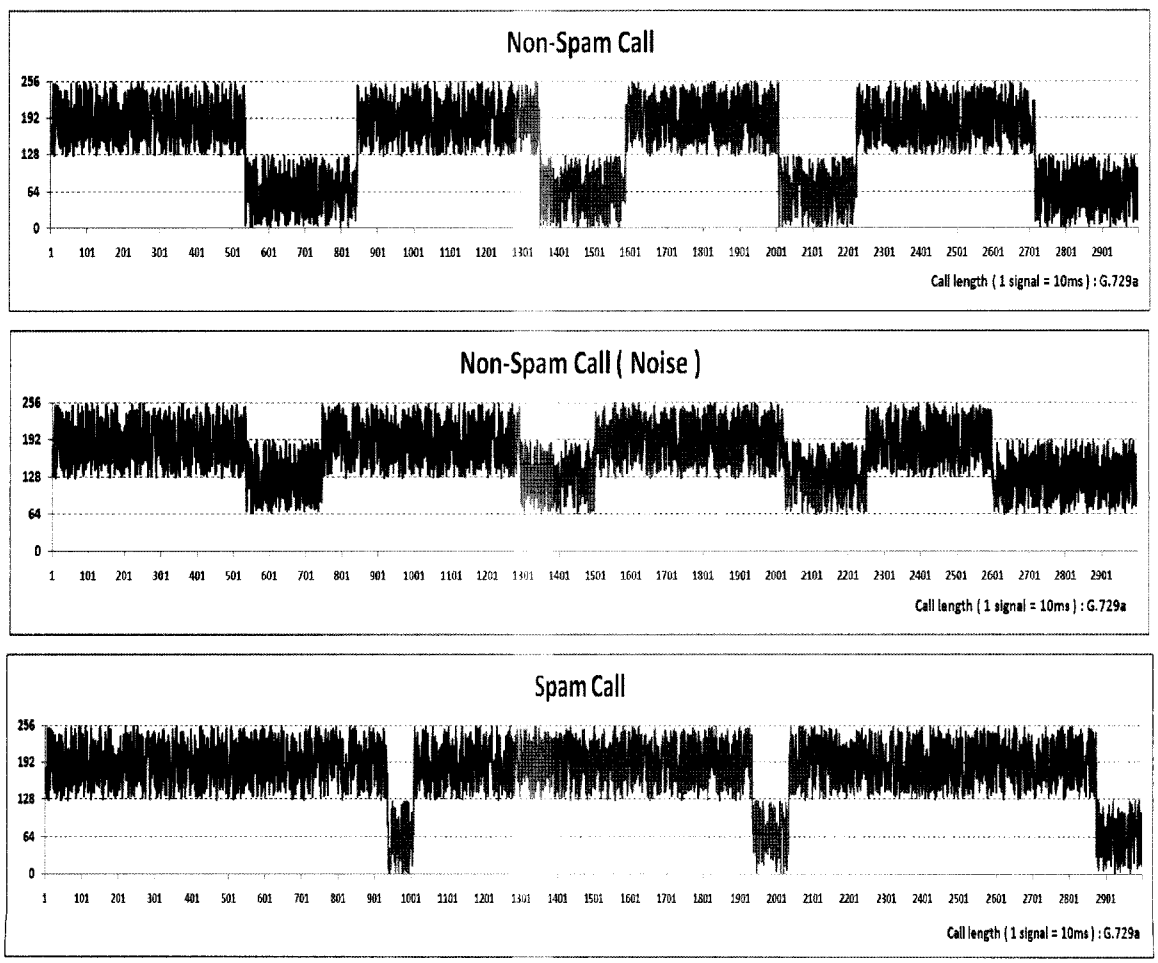
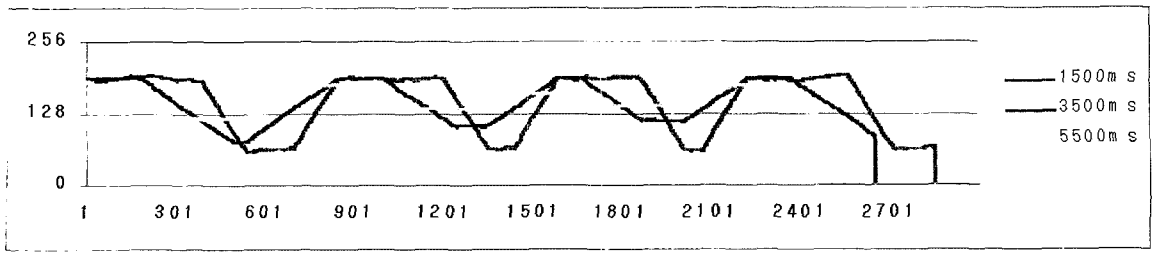
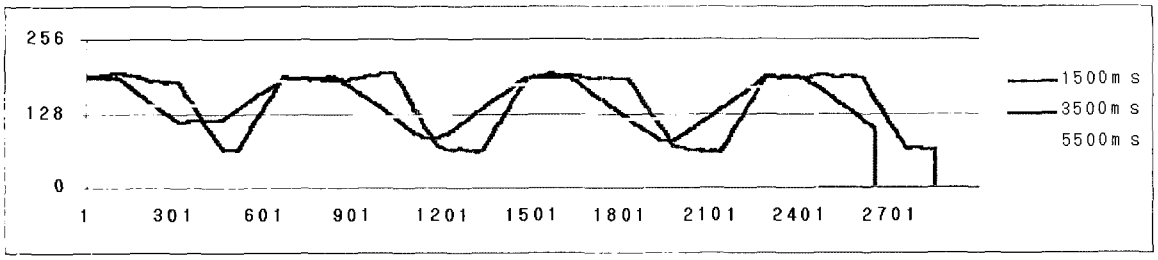


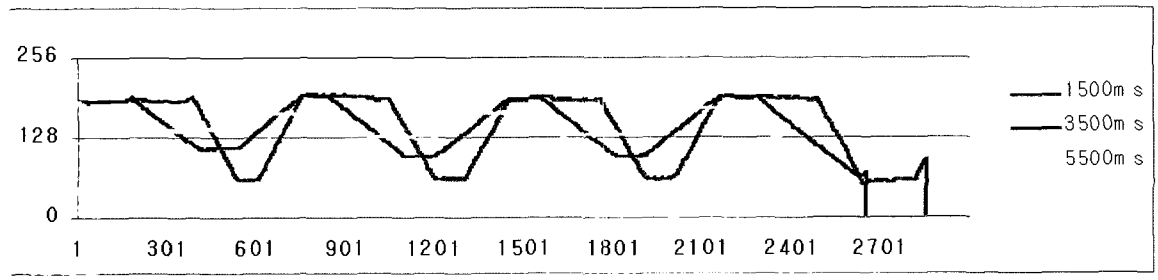
그림 6. Non-Spam Call, Noise Call, Spam Call 모델 음성 신호 그래프



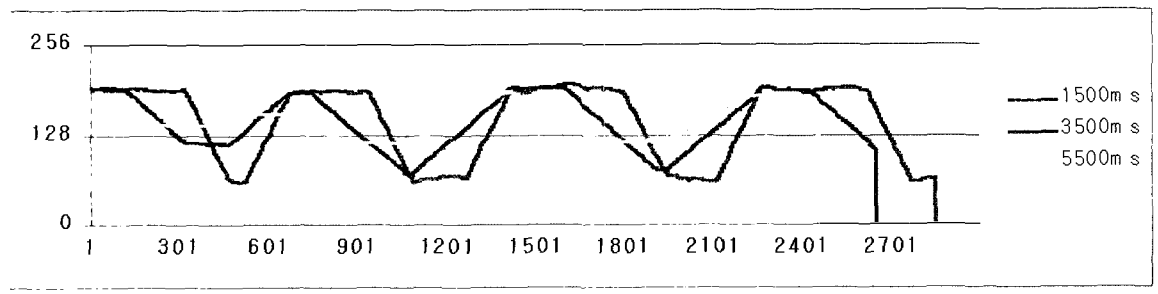
seed 1



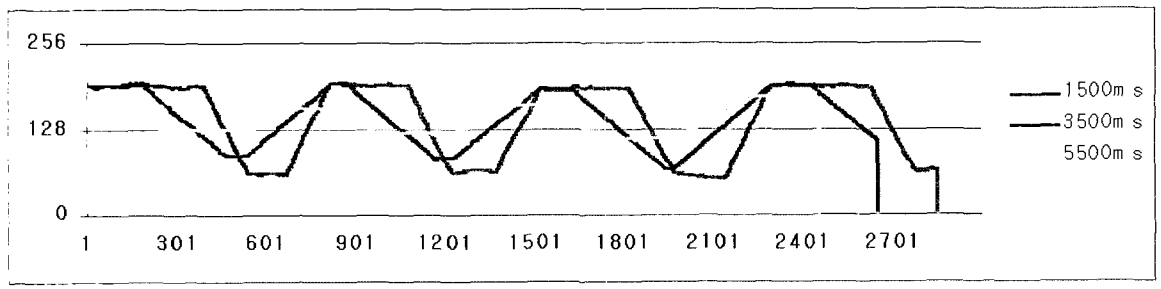
seed 2



seed 3

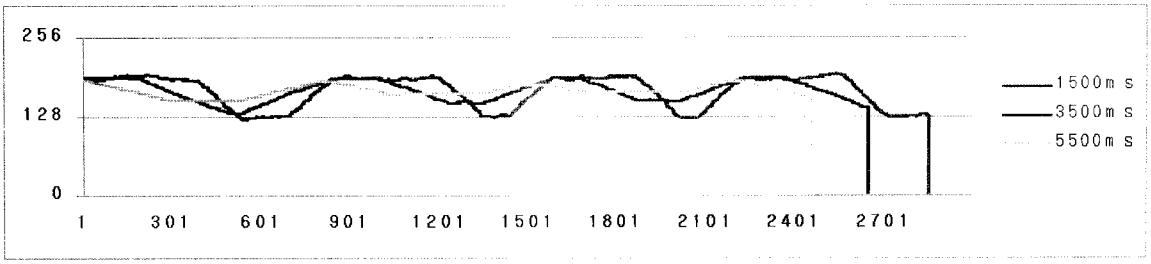


seed 4

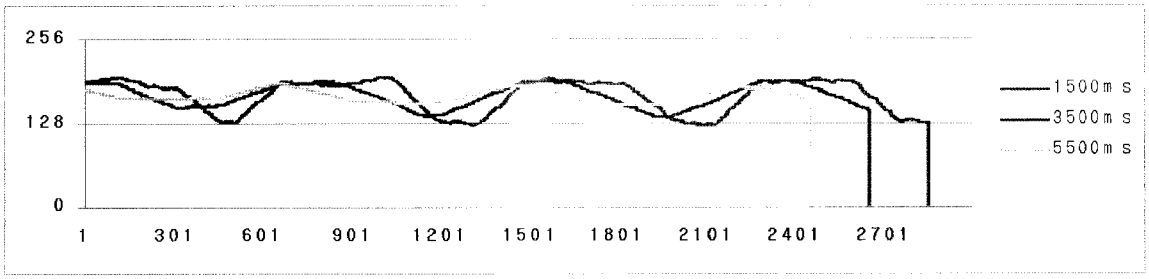


seed 5

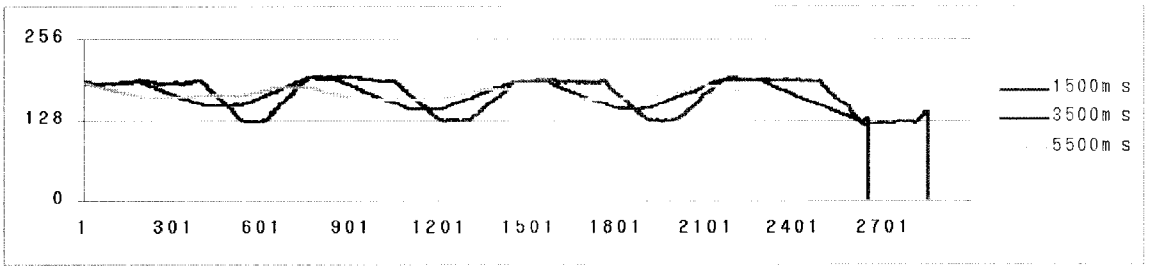
그림 7. Non-Spam Call 모델 결과 그래프



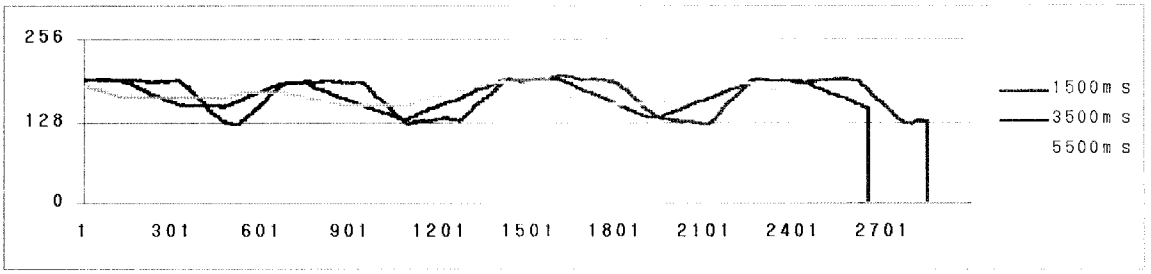
seed 1



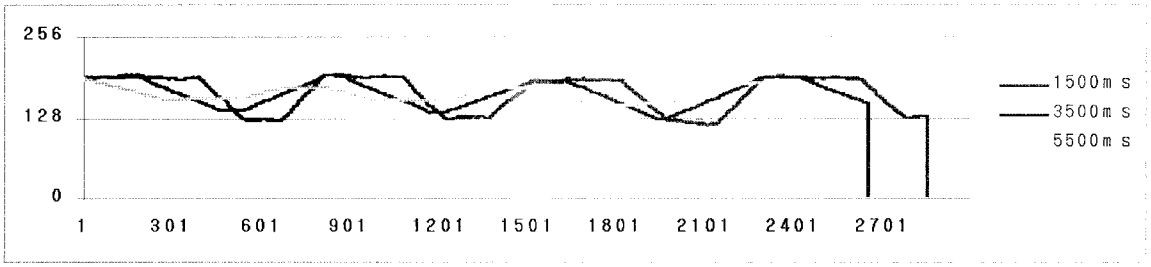
seed 2



seed 3

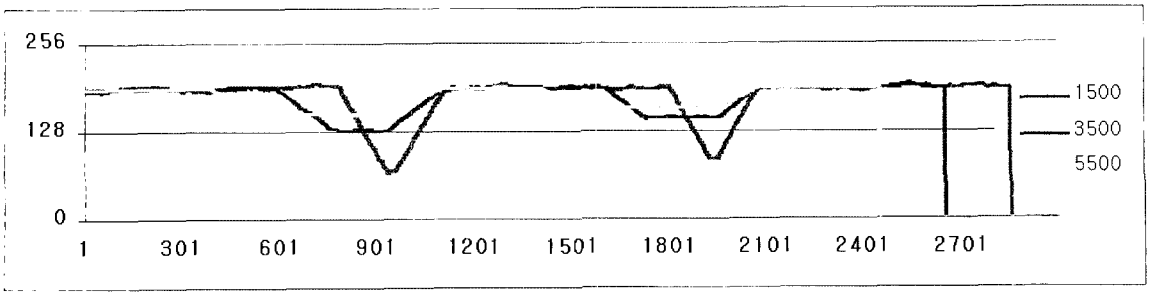


seed 4

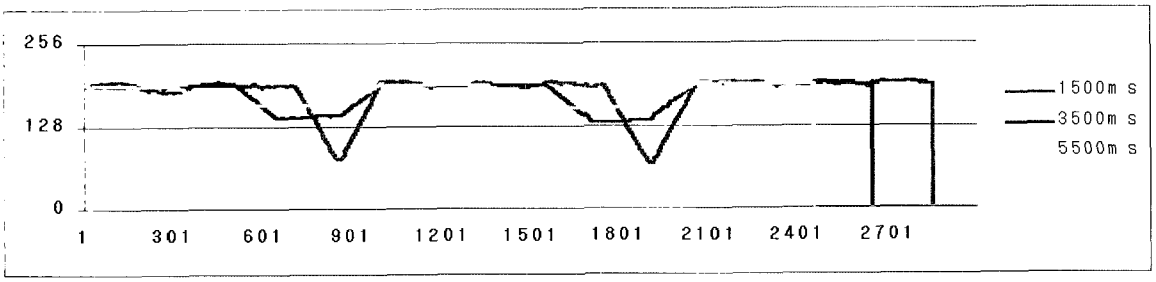


seed 5

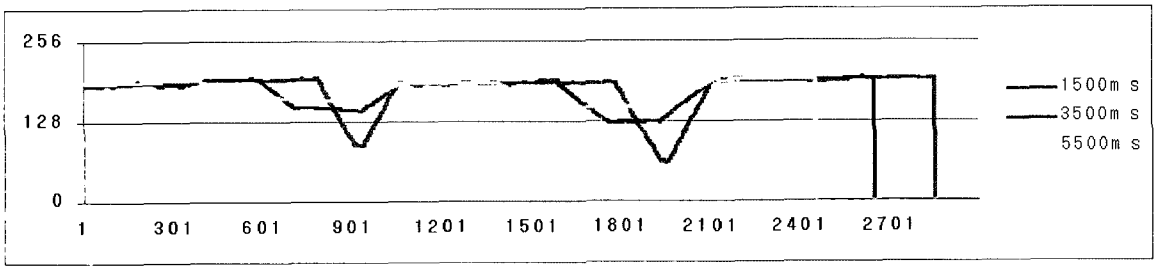
그림 **8.** Noise Call 모델 결과 그래프



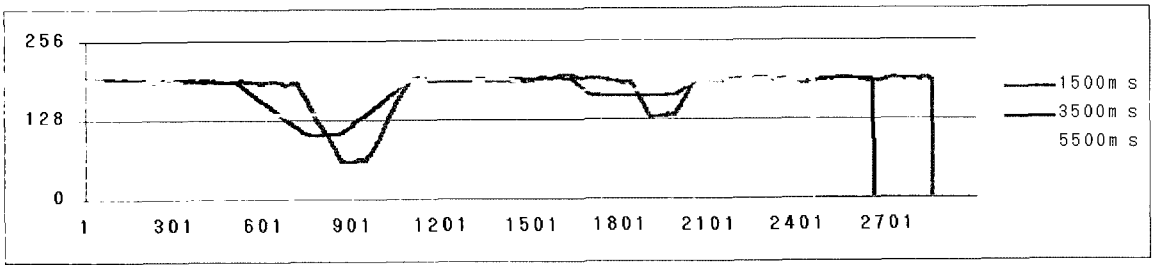
seed 1



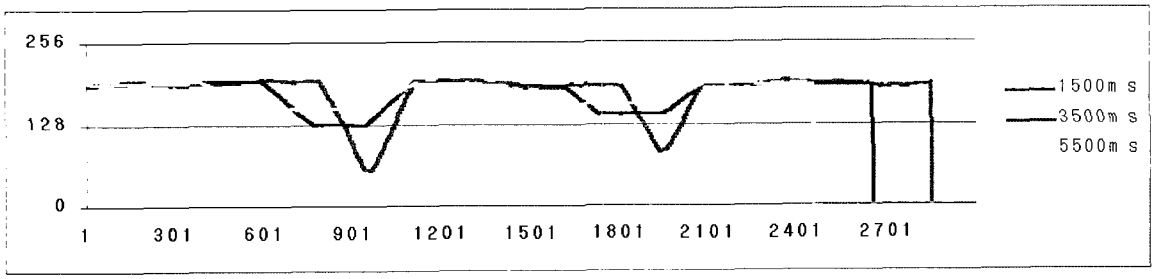
seed 2



seed 3



seed 4



seed 5

그림 **9.** Spam Call 모델 결과 그래프

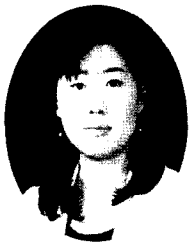
Spam Call 모델의 시뮬레이션을 수행 한 결과, 분석 단위 시간을 1500ms로 설정하였을 경우에는 콜이 5가지 seed값에 대하여 모두 Non-Spam으로 결정된 것을 볼 수 있다. 이것은 1500ms가 Spam Call 모델의 meaningless message 전송 구간 사이에 존재하는 값이기 때문에 나올 수 있는 결과이다. 분석 단위 시간이 3500ms인 경우에는 seed값이 3, 4, 5일 때 Non-Spam으로 결정되었고, 이 경우에도 평균이 각각 127, 124, 126이상인 것을 보면 근소한 차이로 Non-Spam으로 결정되었음을 알 수 있다. 또 분석 단위 시간이 5500ms인 경우에는 seed값에 상관없이 모두 Spam으로 결정되었다. 이와 같이 스팸 콘텐츠가 짧은 meaningless message 전송 구간을 가지고 있다하더라도 이것이 Spam Call을 Non-Spam Call로 인식하도록 영향을 미치는 것을 보면, 스팸 콘텐츠의 meaningless message 전송 구간 탐지의 중요성을 알 수 있다. 또 이를 위해서는 여러 경우의 스팸 콘텐츠의 패턴을 분석하여 분석 단위 시간을 적절히 설정 할 수 있도록 해야 할 것이다.

5. 결론 및 향후 연구계획

본 논문은 그레이리스트 기반의 VoIP 콜 스팸 탐지 알고리즘을 제시하고 이를 DEVS 형식론을 적용한 모델로 설계하여 콜의 속성별로 검증하였다. 전송되는 VoIP 콜의 음성 신호가 어떠한 의미를 가지고 있는지 판단하는데 있어서 가장 중요한 요소는 분석 단위 시간과 스팸의 기준값을 선정하는 것이고, 실제로 이 요소의 값이 변화함에 따라 같은 콜에 대한 알고리즘의 검증 결과가 달라지는 것을 확인 할 수 있다. 따라서 다양한 경우의 입력 값에 대해서 알고리즘이 갖는 동적인 특성을 분석하여 알고리즘을 조율하는 작업이 필요하고, 이 알고리즘을 토대로 그레이리스트를 관리하기 위한 정책을 마련해야 할 것이다.

참 고 문 헌

1. 정수환, "VoIP 스팸과 보안", TTA Journal Vol. 104J, 2005.
2. KISA, "인터넷 이메일 스팸 차단 방식 분석".
3. KISA(인터넷 침해 사고 대응 지원 센터), "SPF기술설명서", 2005.
4. Ram Dantu, Prakash Kolan, "Detecting Spam in VoIP Networks", 2005.
5. D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, "Security Considerations for Voice Over IP Systems", Technical Report, NIST, SP800-58.
6. Voice Over Internet Protocol (VoIP) Security Technical Implementation Guide, Defense Information System Agency DISA, Jan 2004.
7. Mehran Sahami, Susan Dumais, David Heckerman, and Eric Horvitz, "A Bayesian Approach to Filtering Junk E-Mail", Proceedings of AAAI 1998 Workshop on Learning for Text Categorization, Madison, Wisconsin, USA, pp. 55-62, 1998.
8. 이미라, "계층적 계획을 이용한 이산 사건 시뮬레이션 모델링: HRG-DEVS", 한국시뮬레이션학회 논문지 Vol. 15, No. 2, pp. 1-12, 2006.
9. Zeigler, B.P., Praehofer, H. and Kim, T.G., "Theory of Modeling and Simulation: Integrating Discrete Event and Continuous Complex Dynamic Systems", Academic Press, 2000.
10. 강원석, 김기형,"분산 시뮬레이션을 위한 DEVS 특성 기반 시뮬레이션 모델 분배 방법", 한국정보과학회 학술발표논문집 Vol. 34, No. 1 pp. 513-518, 2007.
11. Vijay Balasubramaniyan, Mustaque Ahamad, Haesun Park, "CallRank: Combating SPIT Using Call Duration, Social Networks and Global Reputation", 2007.
12. Yufen Jiang, "Performance evaluation of SIP based voice conferencing over the IEEE 802.11 wireless networks", 2003.
13. 이인희, 박대우, "VoIP 서비스의 스팸 공격에 대한 차단 연구 2006", 한국컴퓨터정보학회 논문지 Vol. 11, No. 5 pp. 241-250, 2006.
14. 김윤배, 이계신, 김재범,"자기유사성을 고려한 VoIP 트래픽 생성 시뮬레이션 방법의 연구", 한국시뮬레이션학회 2004년 춘계학술대회논문집 pp. 25-29, 2004.
15. 김중민, "MPLS를 적용한 망에서 VoIP 서비스의 지연 특성 개선", 2005.
16. 김형석,"VoIP에서 음성 코덱이 QoS에 미치는 영향", 2002.
17. 윤상윤, 정진욱,"VoIP 상에서 다양한 응용 서비스 트래픽에 따른 종단간 사용자의 음성 트래픽 지연 변화 연구", 한국시뮬레이션학회 논문지 Vol. 10 No. 2 pp. 15-24, 2001.



김 지 연 (jjia1230@swu.ac.kr)

2007년 2월 서울여자대학교 정보보호공학과 공학사
2007년 3월~현재 서울여자대학교 컴퓨터학과 석박사통합과정

관심분야 : 정보보안, VoIP 보안, 모델링&시뮬레이션

김 형 종 (hkim@swu.ac.kr)

1996년 성균관대학교 정보공학과 공학사
1998년 성균관대학교 정보공학과 공학석사
2001년 성균관대학교 전기전자 및 컴퓨터공학과 공학박사
2001년~2007년 한국정보보호진흥원 수석연구원
2004년~2006년 미국 카네기멜론대학 CyLab Visiting Scholar
2007년~현재 서울여자대학교 컴퓨터학부 전임강사

관심분야 : 취약점 분석 및 모델링, 이산사건 시뮬레이션 방법론, 침입감내기술

조 영 덕 (ydcho@kisa.or.kr)

2000년 2월 아주대학교 정보및컴퓨터공학부 졸업
2002년 2월 아주대학교 정보통신공학과 석사
2002년~현재 한국정보보호진흥원 IT기반보호단 응용기술팀

관심분야 : VoIP 보안, 신종스팸 대응, 네트워크 보안, 신규IT서비스 보안

김 환 국 (rinyfeel@kisa.or.kr)

1992년 3월~1998년 2월 한국항공대학교 전자계산학과 이학사
1998년 3월~2000년 8월 한국항공대학교 대학원 컴퓨터공학과 공학석사
2002년 4월~2006년 12월 ETRI 정보보호연구단 연구원
2007년 1월~현재 한국정보보호진흥원 IT기반보호단 선임연구원

관심분야 : 네트워크 보안, VoIP 보안, 정보보호

원 유 재 (yjwon@kisa.or.kr)

1985년 2월~충남대학교 계산통계학과 학사
1987년 2월~충남대학교 계산통계학과 석사
1998년 8월 충남대학교 전산학과 박사
1987년 2월~2001년 2월 한국전자통신연구원 팀장
2001년 3월~2004년 8월 안랩유비웨어 연구소장
2004년 9월~현재 한국정보보호진흥원 IT기반보호단 응용기술팀 팀장

관심분야 : 멀티캐스트 보안, 무선통신 보안, IPv6 보안, 멀티미디어, 콘텐츠 보안, 신규IT서비스 보안

김 명 주 (mjkim@swu.ac.kr)

1986년 2월 서울대학교 컴퓨터공학과 공학사
1988년 2월 서울대학교 컴퓨터공학과 공학석사
1993년 8월 서울대학교 컴퓨터공학과 공학박사
1993년 9월~1995년 8월 서울대학교 컴퓨터 신기술 공동연구소 특별연구원
2003년~2004년 미국 펜실바니아대학교(UPenn) 객원 연구원
1995년~현재 서울여자대학교 컴퓨터학부 교수

관심분야 : 정보보안, USN, 의료정보, 콘텐츠보안