VoIP 스팸과 보안

정 수 환 숭실대학교 정보통신전자공학부

1. 개요

VoIP(Voice over Internet Protocol)는 컴퓨터 네트워크 환경에서 음성 데이터를 인터넷 프로토콜 데이터 패킷으로 변환하여 일반 PSTN에서의 음성통화와 똑같은 서비스를 제공한다. VoIP 시그널링의 종류에는 ITU-T의 H.323과 IETF의 SIP(Session Initiation Protocol)가 있다.

지금까지는 H.323 기반의 VoIP 서비스 개발이 많이 이루어져 왔으나 최근에는 SIP기반의 VoIP 서비스 개발이 활발하게 진행 중에 있다. SIP는 파싱과 컴파일이 쉽고 확장성이 뛰어나며 문자기반이기 때문에 H.323에 비해서 구현이 용이한 장점을 가지고 있다.

SIP를 기반으로 하는 VoIP 서비스의 장점과 이에 대한 기업들의 관심이 증가하면서 VoIP에 대한 보안의 중요성이 제기되고 있다. 그 중 VoIP 스팸은 현재 우리가 경험하고 있는 이메일 스팸과 비슷한 형태로써 원하지 않는 음성, 메시지, 전화통화를 전달하여 서비스 이용을 불편하게 만든다. 기존의 텔레마케팅 회사들은 일반 전화(PSTN)를 사용할 경우 하나의 콜(Call)을 생성하기 위해서는 오직 한 개의 전화선만을 사용할 수 있으며, 하나의 콜에 대한 사용요금을 지불해야 하기 때문에 비용적인 측면에서 부담이 컸다. 하지만 VoIP 스팸을 이용하면 한 번에 수천 개의 주소에 같은 메시지를 보낼 수 있으며 기존 네트워크망을 이용하기 때문에 비용적인 부담을 줄일 수 있다. 따라서 스패머는 PSTN에서의 요금에 대한 부담을 줄이고 VoIP 서비스 환경에서 저렴한 비용으로 상업적인 광고나, 악의적인 스팸을 보낼 수 있는 보안의 취약성이 발생하게 된다.

본 고에서는 VoIP 스팸에 대한 정의와 VoIP 스팸 기술에 대한 분석 그리고 VoIP 스팸을 막을 수 있는 여러 가지 대응방법들에 대해서 설명을 하도록 한다.

2. VoIP 스팸의 정의와 종류

스팸(spam)이란 '원치 않는 비상업적 혹은 상업적으로 사업적 관계를 갖지 않는 사람이 보낸 모든 통신'을 말한다. 스팸은 일방적이고 대량으로 보내지는 메시지로 인터넷 이메일이 대표적이다. SIP는 IP 기반 네트워크에서 통신을 위한 시그널링 프로토콜로 자리잡고 있으므로, 이메일 스팸과 같이 SIP 기반의 시스템에서도 스팸이 발생할 수 있다. 이번 절에서는 SIP 기반의 VoIP 스팸에 대한 정의를 Call 스팸, IM 스팸, Presence 스팸과 같이 세 가지로 분류하여 설명하고 각각의 스팸에 대한 특징을 분석한다.

2.1 Call 스팸

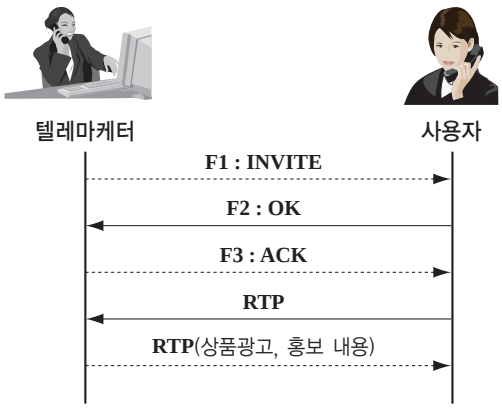

그림 1. 콜 스팸 사례

Call 스팸은 SIP INVITE 메시지를 임의의 사용자들에게 음성, 비디오, 인스턴트 메시지 등의 통신을 위해서 대량으로 전송한 후, 세션을 시도하는 방법이다. VoIP 환경에서의 Call Spam에 대한 가능성을 의심해 볼 수 있겠지만, Call 스팸은 현재 PSTN 망에서 텔레마케팅과 같은 형태로 나타날 수 있다. 예를 들면, 텔레마케터(spammer)가 랜덤하게 선택된 사용자들에게 SIP INVITE를 통해 전화를 걸고, INVITE를 수신한 사용자가 응답을 하여 세션이 이루어지면 텔레마케터는 불필요한 광고를 할 수 있게 된다.

Call 스팸과 이메일 스팸은 불필요한 정보를 전송함으로써 서비스 이용을 불편하게 하는 공통점이 있지만, Call 스팸은 이메일 스팸과 달리 대량으로 발송되지 않는다. 이메일 스팸은 시간적인 측면과 비용 측면에서 대량의 메일을 효율적으로 보낼 수 있지만, Call 스팸은 텔레마케터를 고용하는 비용, 사용자들에게 직접 통화를 시도해야 하는 불편함, 그리고 단위 Call 당 비용문제가 발생하기 때문에 spammer에게는 비효율적이다. 그러나 SIP 기반의 VoIP 시스템에서는 이러한 비용문제를 크게 절감할 수 있다. SIP Call 스팸 기술은 소프트웨어 기술이기 때문에 쉽게 구현될 수 있으며 누구나 쉽게 자동화 할 수 있다. spammer는 SIP UAC들에게 동시에 INVITE 메시지를 발송하여 통화를 시도하고, 사용자가 통화 시도에 응답하면 자동으로 ACK 메시지를 생성하여 세션을 성공적으로 성립시킨다. 통화가 이루어지면 spammer는 미리 녹음된 음성 메시지를 통해 수많은 사용자에게 손쉽게 내용을 전달할 수 있다. Call 스팸의 단위 콜 당 비용은 IP 기반의 네트워크 통신을 이용하기 때문에 PSTN의 전화비용보다 저렴하고, VoIP 스팸 기술은 소프트웨어적인 기술이기 때문에 바이러스와 같이 다른 시스템(좀비 시스템)을 이용하여 비용을 크게 절감할 수 있다. 또한 SIP 기반의 VoIP는 이메일 주소를 사용하기 때문에 기존의 이메일 주소 수집 프로그램을 이용하여 이메일 스팸 규모의 사용자들에게 랜덤하게 통화를 시도할 수 있다.

2.2 IM 스팸

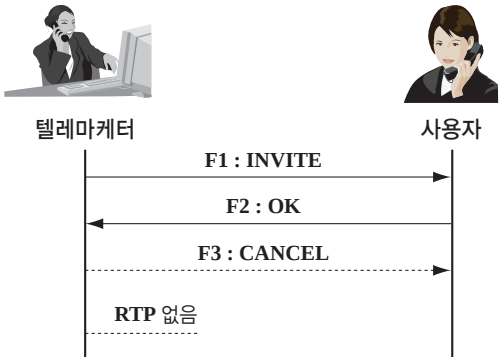

그림 2. 인터넷전화 콜 스팸 사례

인스턴트 메시지 스팸 사례

MESSAGE sip:car@gangnam.domain.com SIP/2.0
Via : SIP/2.0/UDP gangnam.domain.com
From : 광고자@어느자동차학원.com
To : 학생@어떤대학교.ac.kr
Cseq : 1 MESSAGE
Content Type : text/plain
Content Type : 30

"안녕하세요. XXX 자동차 학원입니다. 속성과정을 신청하시면 1주일 안에 면허증 취득이 가능합니다.

그림 3. 인스턴트 메시지 스팸

IM(Instant Messaging) 스팸은 이메일 스팸과 유사한 형태의 스팸 기술로 그림 2와 같은 방법을 사용하여 일방적이고 대량으로 전송하는 인스턴트 메시지이다. 이 스팸 기술은 IM을 위한 확장된 SIP 메시지를 사용하여 이루어지지만 INVITE, OPTION, SUBSCRIBE와 같은 일반적인 SIP Request 메시지들의 Subject 헤더를 이용하여 그림 3과 같이 송신자에게 자동으로 불필요한 문구를 보여줄 수 있다. IM 스팸은 이메일 스팸과 매우 유사한 형태이고 소요되는 비용도 비슷하지만 이메일 스팸보다 더 큰 영향력이 있다. 이메일 스팸은 사용자가 메일을 보는 동작에 의해서 나타나거나 바로 삭제가 가능하지만 IM 스팸은 자동적으로 팝업 되기 때문에 모든 스팸 정보가 사용자에게 나타날 수 있다. 그러나 IM 시스템의 대부분이 화이트 리스트(white lists)를 사용하여 메시지를 주고받기 때문에 IM 스팸이 실제 환경에서 큰 영향력은 없다.

2.3 Presence 스팸

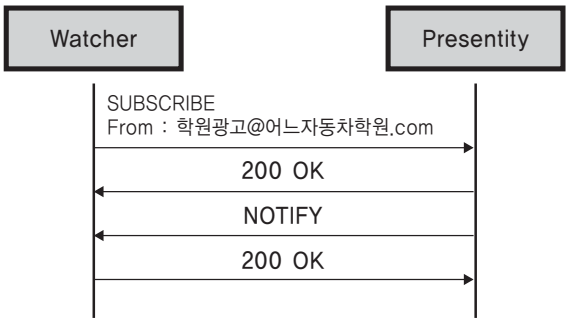

그림 4. Presence 스팸 사례

프리젠스 스팸은 IM 스팸 기술과 유사한 기술로 일방적이고 대량으로 보내지는 프리젠스 요청 메시지이다. 이 스팸 기술은 IM 메시지를 보내거나 다른 형태의 통신을 하기 위해 사용자의 "버디 리스트" 또는 "화이트 리스트"의 획득을 목적으로 SIP 메시지인 "SUBSCRIBE" 요청 메시지를 사용하는 기술이다. 대부분의 프리젠스 시스템들이 동의 기반의 프레임워크를 제공하기 때문에 프리젠스 스팸의 영향력은 미비하다. 사용자들의 프리젠스를 볼 수 있는 권한이 없는 와쳐(Watcher)는 그들의 프리젠스 정보를 얻을 수 없다. 그러나 프리젠스 요청 메시지는 일반적으로 사용자에게 전달되고, 사용자로부터 승인을 받거나 거절을 당하는 구조로 되어 있다. SIP에서 이러한 기능은 watcherinfo event package로 사용된다. 이 패키지는 사용자에게 watcher의 식별자(identity)를 확인하여 승인하거나 거절할 수 있도록 한다. SIP의 이런 특성을 이용하여 spammer는 사용자들에게 필요한 정보를 간략하게 보여줄 수 있다. 예를 들면, sip:please-buy-my-product@spam.example.com과 같은 형태의 SUBSCRIBE 메시지를 사용자에게 보내면 사용자에게 요청 메시지에 대한 승인을 얻기 위해 자동적으로 보여질 것이다. 프리젠스 스팸은 IM 스팸과 같이 정보를 전달한다는 점은 비슷하지만 전달할 수 있는 정보의 양이 제한되어 있다는 차이점이 있다.

3. VoIP 스팸 대응기술

3.1 Contents 필터링

이메일 스팸에서 사용되는 가장 일반적인 형태의 스팸 대응 기술이다. 스팸 필터는 이메일의 콘텐츠를 분석하고 내용을 파악하여 스팸 정보를 걸러내는 방식이다. 대표적인 Contents 필터링으로 베이지언(Bayesian) 스팸 필터가 있다. 그러나 콘텐츠 필터링 방식은 Call 스팸의 경우 다음과 같은 두 가지 이유로 완벽한 해결책이 못된다. 첫째, 전화가 왔을 경우 사용자는 전화를 받기 전까지는 콘텐츠의 내용을 파악할 수가 없다. 콘텐츠는 통화를 시작하면서부터 전달되기 때문에 콘텐츠를 파악하여 필터링을 하기에는 부적절하다. 둘째, 음성 메일(voicemail) 형태와 같이 콘텐츠가 음성, 비디오로 되어 있을 경우 음성 및 비디오 인식기술이 현재까지 정교하지 않기 때문에 콘텐츠를 분석하여 스팸인지 아닌지 판단하는데 어려움이 있다. 또한 음성 패턴을 파악하여 스팸에 대한 필터링을 수행할 수 있지만, spammer는 사용자에게 정보를 전달하는데 지장이 없을 정도의 잡음을

발생시킴으로써 콘텐츠 분석을 난해하게 할 수 있다. 콘텐츠 필터링 기술은 Call 스팸보다는 이메일 스팸과 유사한 IM 스팸 대응 기술로 적합하다.

3.2 Black 리스트

블랙리스트는 spammer의 주소를 리스팅 하여 주소 매핑에 의해 스팸을 차단하는 방식이다. 리스트에 포함되는 주소는 이메일 주소(spammer@domain.com) 또는 도메인 전체 이름(spammers.com)으로 설정할 수 있다. 단순한 블랙리스트는 이메일 스팸에 대해서 다음과 같은 두 가지 이유로 효율성이 떨어진다. 첫째, 이메일 주소는 쉽게 스푸핑(spoofing)될 수 있으며 spammer는 스푸핑된 주소를 사용하여 다른 사람으로 위장할 수 있다. 만약 spammer가 블랙리스트에 없는 임의의 주소를 사용하여 메일을 보낸다면 블랙리스트는 무용지물이 된다. 둘째, 이메일 주소를 위조해서 사용하지 않더라고 이메일 주소는 얼마든지 새로 생성할 수 있다. 하나의 도메인 내에서 생성할 수 있는 이메일 아이디의 수는 무제한이며, 하나의 도메인을 생성하여 사용하는 비용도 저렴하다. spammer의 이메일 주소가 사용자의 블랙리스트에 등록되면 spammer는 새로운 이메일 주소를 생성하여 스팸 정보를 보낼 수 있고 다음(Daum), 야후(Yahoo)와 같은 이메일 서비스 제공업체의 도메인을 이용하여 스팸 정보를 보낸다면 블랙리스트의 도메인 전체 이름을 통한 필터링도 불가능하다. 결과적으로 이메일 아이디가 쉽게 생성될 수 있기 때문에, 블랙리스트를 통한 스팸 대응은 큰 효과를 기대하기 힘들다.

3.3 White 리스트

화이트 리스트는 블랙 리스트의 반대 방식으로 유효한 사용자의 이메일만 받아들인다. 화이트 리스트 방식은 스푸핑된 주소를 사용하여 사용자의 화이트 리스트에 등록될 수 있지만, 강력한 아이디 인증방법을 사용하여 이러한 문제를 예방할 수 있다. 결과적으로 화이트 리스트와 사용자에 대한 인증방법이 함께 사용되어야만 스팸 대응에 효과가 있다. 그러나 화이트 리스트 방식은 “introduction problem”이 있다. 정당한 송신자가 사용자에게 처음으로 통신하고자 할 경우에 화이트 리스트에 없기 때문에 통신을 할 수 없는 문제이다. 정당한 사용자의 통신요청과 spammer의 스팸 정보를 구별하는 것은 쉽지 않다. 인터넷 메신저와 같은 IM 시스템에서는 화이트 리스트가 유용하게 적용될 수 있다. 메신저는 화이트 리스트와 같은 버디 리스트를 기본적으로 제공하기 때문에 리스트에 등록된 사용자와의 메시지 교환이 가능하며, “introduction problem”도 메신저에서는 상대방의 버디 리스트에 등록하기 위해서는 “동의”를 통해서 이루어지기 때문에 기본적으로 화이트 리스트를 사용한 효과를 볼 수 있다. 또한 IM 시스템은 인증 메커니즘이 제공되어 화이트 리스트 방식의 문제점을 해결할 수 있다.

IM 시스템에 효과적인 화이트 리스트는 SIP에 적용할 수 있다. SIP 표준에 버디 리스트 개념과 프리젠스 시스템이 명시되어 있기 때문에 SIP 시스템에 적용하여 효과적으로 스팸에 대응할 수 있다. 이와 같이 화이트 리스트는 SIP 스팸에 적용할 수 있지만 여전히 “introduction problem”이 남아 있다. 화이트 리스트 방식이 SIP 스팸에 효과적인 스팸 대응 기술이 되기 위해서는 “introduction problem”을 해결할 수 있는 방법과 같이 사용되어야 한다.

3.4 Consent-based 통신

동의 기반(consent-based) 시스템은 블랙 또는 화이트 리스트와 함께 사용된다. 예를 들면, 사용자 Alice가 Bob과 통신할 때, Bob의 블랙 또는 화이트 리스트에 Alice에 대한 정보가 없기 때문에 초기 통신과정은 거절되고, 동의를 요청한다. 이후에 다시 Alice가 Bob에게 통신을 시도하면 Bob은 Alice가 이전에 통신을 시도 했다는 것을 알고 Alice의 요청을 승낙하거나 거절한다. 이러한 동의기반 시스템은 프리젠스와 IM 시스템에서 폭넓게 사용되고 이메일 시스템에서는 사용되지 않는다.

SIP는 동의기반 시스템의 프리젠스, watcher information event package와 같이 누가 가입을 했는지 사용자가 알 수 있도록 표준에 명시되어 있다. 그러나 동의기반 시스템은 IM 또는 전화 시스템에서는 효과적이지 않다. 동의기반 시스템이 IM 또는 전화 시스템에 효과적인 것처럼 보이지만 스팸의 근본적인 특성만 바뀔 뿐이다. 스팸의 콘텐츠를 통해 불필요한 정보를 받는 것을 막을 수는 있지만, 동의요청에 의해 사람을 성가시게 하는 것은 막을 수 없다.

3.5 Reputation 시스템

평판(reputation) 시스템은 화이트 또는 블랙리스트와 함께 사용된다. 평판 시스템은 요청자의 아이디에 대한 spammer에 대한 구별을 평판도(reputation score)를 사용하여 판단하도록 한다. 예를 들면, Alice의 블랙 또는 화이트 리스트에 Bob이 등록되어 있지 않은 상태에서 Bob이 Alice에게 요청을 하면 Bob의 평판도가 Alice에게 보여지고, Alice는 평판도의 점수를 보고 요청에 대한 수락여부를 판단한다. 일반적으로 평판 시스템은 중앙집중식 메시지 전송구조에서 구현되며, 실제 오늘날 하나의 메시지 서비스 제공업체에서 통합적으로 관리하는 구조로 이루어져 있다. 평판도는 사용자에게 요청받은 메시지에 대해서 스팸 정보라고 판단되면 중앙 시스템에 spammer의 아이디어를 신고하는 방식이다. 예를 들면, 사용자가 애플리케이션 프로그램에서 버튼을 누르게 되면 spammer 아이디가 중앙 평판 시스템에 전송된다. 몇몇의 사용자만이 신고한 아이디를 spammer로 판단하기는 어렵지만, 연속적인 또는 다량의 신고를 받은 아이디에 대해서 spammer로 판단하는 것은 가능하다. 평판 시스템은 중앙집중식 메시지 서비스 시스템에서 구현되어야 효과적이기 때문에 서로 다른 서비스 시스템이 공존하는 현실에서는 큰 효과를 볼 수 없다.

평판도 시스템은 Negative 평판도와 Positive 평판도 시스템으로 분류할 수 있다. Negative 평판도를 기반으로 하는 평판 시스템은 블랙리스트와 동일한 문제점을 갖는다. 만약 아이디를 쉽게 얻거나 생성할 수 있다면 평판도가 낮은 아이디는 버리고 새로운 아이디를 사용할 수 있다. 또한 공모에 의해서 누구든지 나쁜 평판도를 받을 수 있다. Positive 평판도를 기반으로 하는 평판 시스템도 Negative 평판도 시스템과 동일한 문제점을 가지고 있다. 다량의 아이디를 소유한 spammer가 칭찬을 통해 어느 특정 아이디에 대해서 평판도를 높여 스팸에 사용할 수 있기 때문이다.

3.6 Legal Action

Legal Action 방식은 국가에서 스팸을 보내는 업체 및 개인에게 법적인 제재를 가하는 것이다. 이 방식은 이메일 스팸, Call 스팸, IM 스팸 등에서 아주 쉽게 적용할 수 있다. SIP 스팸에 대한 보안을 위해 Legal Action이 실제 스팸을 방지하는데 효과적인지에 대해서 많은 논쟁이 있었지만, 최근 미국에서 있었던 예를 들면, “do not call” 리스트를 사용하여 스팸 방지에 효과가 있었다. 미국 내의 텔레마케팅 업체는 국내의 이러한 법안을 피하기 위해 국제 통화를 이용할 수 있으나 국제 통화 비용의 문제로 미국 내의 사용자들에게 전화를 할 것이다. 만약 텔레마케팅 업체가 미국 내의 국내 통화로 마케팅을 한다면 위치추적이 가능하고, 위법한 행동을 초래하기 때문에 업체들의 스팸 활동을 법안을 통해서 제한할 수 있다. 반대의 예로, VoIP나 이메일에 대해서 “do not irritate” 리스트를 사용한 방법은 전화를 통한 스팸이 아닌 IM 스팸과 이메일 스팸을 사용해서 법망을 피해 발신지가 미국이 아닌 다른 나라에서 저렴한 비용으로 보낼 수 있기 때문에 효과적이지 못하다. 이 문제는 송신자의 아이디를 확실하게 인증하고 이러한 것들이 위법한 행동일 경우에 처리할 수 있는 사법권이 있다면 해결할 수 있다.

4. 결론

지금까지 VoIP 스팸의 종류와 그에 대한 대응 기술들을 살펴보았다. VoIP 스팸에 대한 대응 기술들은 독립적으로 동작하기 보다는 다른 스팸 대응 기술들과 상호보완적으로 동작함으로써 노출되는 보안의 취약성을 막을 수 있었다. 하지만 아직까지 VoIP 스팸에 대한 완벽한 해결책은 제시하지 못하고 있다.

앞으로 VoIP의 발전은 SIP를 기반으로 하는 서비스의 형태로 발전하게 될 것이다. 현재 SIP 프로토콜은 폭넓게 사용되고 있지만, 그 배포 수준은 폐쇄된 네트워크 공간에서 제한적으로 사용되고 있다. 또한 VoIP 서비스를 제공하는 전화 사업자들도 순수 VoIP 망으로 긴밀하게 연결되어 있지 않다. 따라서 공개된 인터넷 망을 사용하여 SIP 메시지를 송수신 하는 것은 극히 제한적인 수준이다. 이러한 환경에서 VoIP 망은 스팸에 심각한 영향을 받고 있지 않다. 하지만, 머지않아 인터넷 망에서 SIP 메시지의 송수신이 자유로워지는 시기가 올 것이고, SIP 기반의 VoIP 스팸에 대한 보안이 동작하지 않는다면 많은 사용자들의 혼란을 초래할 것이다.

본 고에서 SIP 기반의 VoIP 스팸 문제에 대한 많은 해결책이 제시되었지만, 가장 핵심이 되는 해결책은 SIP URL에 대한 인증을 제공하는 것이다. SIP 표준문서 RFC3261에서는 SIP 사용자에 대한 인증 메커니즘으로 HTTP Digest 방법을 사용하여 등록된 사용자에 대해서만 서비스를 이용할 수 있게 하고, "Enhancements for Authentication Identity Management in The SIP"와 같은 Draft 문서를 통해서 다양하고 강화된 인증방법을 제공한다. 현재 SIP를 기반으로 하는 VoIP 스팸에 대한 연구가 활발히 진행 중에 있다.

참고문헌

[1] Campbell, B., Rosenberg, J., Schulzrinne, H., Huitema, C. and D. Gurle, "Session Initiation Protocol(SIP) Extension for Instant Messaging", RFC 3428, December 2002.

[2] Rosenberg, J., "A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)", RFC 3857, August 2004.

[3] Faltstrom, P. and M. Mealling, "The E.164 to Uniform Resource Identifiers(URI) Dynamic Delegation Discovery System(DDDS) Application(ENUM)", RFC 3761, April 2004.

[4] Rosenberg, J., "A Presence Event Package for the Session Initiation Protocol(SIP)", RFC 3856, August 2004.

[5] Clayton, R. and B. Laurie, "Proof of Work Proves not to Work, Third Annual Workshop on Economics and Information Security", May 2004.

[6] Abadi, M., Burrows, M., Birrell, A., Dabek, F. and T. Wobber, "Bankable Postage for Network Services, Proceedings of the 8th Asian Computing Science Conference, Mumbai, India", December 2003.

[7] Peterson, J., " Enhancements for Authenticated Identity Management in the Session Initiation Protocol(SIP)", draft-ietf-sip-identity-03(work in progress), September 2004.

[8] Jennings, C., Peterson, J. and M. Watson, "Private Extensions to the Session Initiation Protocol(SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002.

[9] Rosenberg, J., "A Framework for Consent-Based Communications in the Session Initiation Protocol(SIP)", draft-ietf-sipping-

consent- framework-00(work in progress), October 2004.

[10] C. Jennings, "Computational Puzzles for SPAM Reduction in SIP," draft-jennings-sip-hashcash-02. July, 2005.

[11] J. Rosenberg, G. Camarillo, D. Willis, "Payment for Services in SIP," draft-jennings-sipping-pay-02, July 2005.