튜링 테스트 기반으로 한 VoIP 스팸방지

(Anti-Spam for VoIP based on Turing Test)

김 명 원 † 곽 후 근 ††
(Myungwon Kim) (Hukeun Kwak)

정 규 식 †††
(Kyusik Chung)

요 약 ITSP(Internet Telephony Service Provider)를 이용한 VoIP 서비스의 사용자가 증가함에 따라 VoIP 스팸은 큰 문제로 대두되고 있다. 기존의 일반 전화 때부터 사용되던 스팸은 실시간적 음성 통신이라는 특성상 콘텐츠 필터링을 하기 어렵기 때문에 콜 행위 패턴 조사를 통해 스패머(Spammer)를 구분하고 있다. 그러나 잘못된 오판으로 인한 문제와 스팸으로 인식하는 임계값을 넘지 않는 한도의 스팸 전송, 그리고 여러 사용자가 하나의 번호를 공유하여 사용하는 경우에는 여전히 스팸의 위협이 남아 있다.

이에 본 논문에서는 튜링 테스트를 이용한 VoIP 스팸 방지를 제안한다. 제안된 방법은 송신자에게 튜링 테스트를 거치게 하고, 튜링 테스트를 통과한 사용자만 수신자와 연결이 되는 방식으로 동작한다. 또한 튜링 테스트를 통과한 정상적인 사용자에게는 티켓을 줌으로써 재발신시 거쳐야하는 튜링 테스트의 번거로움을 줄일 수 있다. 제안된 방법은 ASUS WL-500G 무선 공유기 및 Asterisk IP-PBX에서 구현되었고 실험을 통해 제안된 방법의 유효성을 검증하였다.

키워드 : VoIP 스팸, 튜링 테스트, 무선 공유기

Abstract As increasing the user of VoIP service using ITSP(Internet Telephony Service Provider), the VoIP spam becomes a big problem. The spam used in the existing public telephone is detected by using the pattern inspection of call behavior because it is difficult to filter contents for the characteristic of real-time voice communication. However there is a false-positive problem. The threat on spam remains where spam with low threshold can't be detected or users share one number.

In this paper, we propose anti-spam for VoIP based on turing test. The proposed method gives a user turing test and he/she can connect to a receiver if passing turing test. A ticket is given to a user that pass turing test and it reduces overhead of turing test in re-dial. The proposed method is implemented on ASUS WL-500G wireless router and Asterisk IP-PBX. Experimental results show the effectiveness of the proposed method.

Key words : VoIP Spam, Turing Test, Wireless Router

1. 서 론

VoIP Service는 인터넷 망을 통해 음성신호를 실어 나르는 기술로, 기존 회선교환 방식의 일반전화와 달리 인터넷의 근간인 IP 네트워크를 통해 음성을 패킷 형태로 전송한다. 이러한 VoIP Service는 두 분류로 구분된다[1].

- ITSP VoIP Service
  ex) Samsung070, Mylg070
- Peer to Peer VoIP Service
  ex) Skype

VoIP 기술은 PSTN 망을 사용하는 일반전화보다 저렴한 사용료, 다양한 부가 서비스, 쉬운 설치라는 장점을 가지고 있으며 차세대 망의 구성에 부합하기에 사용자가 증가하고 있다.

1.1 VoIP Spam

VoIP Spam이란 VoIP 서비스에 연관되어 생성되는 Spam이다. 일반 전화와 달리 VoIP Service는 인터넷에 기반을 두고 있어 스팸 공격의 가능성이 매우 높다. 종류로는 크게 다음과 같은 스팸들이 존재한다[2].

- 전화 스팸(Call Spam)
- 인스턴트 메시징 스팸(Instant Messaging Spam)
- 프레즌스 스팸(Presence Spam)

전화 스팸이란 미리 녹음된 광고음성을 프로그램된 기기를 이용하여 대량으로 불특정 다수에게 전송하는 것으로서 기존의 일반전화 시스템에서도 사용되던 Spam의 한 종류이다. 이러한 Call Spam은 Spammer의 입장에서 VoIP Service를 사용하여 더욱 저렴한 가격에 이용가능하며, 실시간 통신을 전제로 하기에 Spam 차단기술의 적용에 어려움이 있다.

· 이 논문은 제34회 추계학술대회에서 '튜링 테스트 기반의 VoIP 스팸방지'의 제목으로 발표된 논문을 확장한 것임
· 본 연구는 한국과학재단 특정기초연구(R01-2006-000-11167-0) 지원으로 이루어졌음.

† 학생회원 : 숭실대학교 정보통신전자공학부
king@q.ssu.ac.kr
†† 정 회 원 : 숭실대학교 정보통신전자공학부 postdoc
gobarian@gmail.com
††† 종신회원 : 숭실대학교 정보통신전자공학부 교수
kchung@q.ssu.ac.kr

논문접수 : 2007년 12월 6일
심사완료 : 2008년 2월 20일

정보과학회논문지: 컴퓨팅의 실제 및 레터 제14권 제3호(2008.5)

인스턴트 메시징 스팸이란 SIP Message 요청 헤더를 사용하여 광고성 내용을 전달하는 Spam 공격이다. 이러한 메시지 요청 외에도 사용자의 화면에 자동으로 광고 내용을 표시되게 하는 다른 요청 헤더를 사용해 사용자를 불편하게 할 수 있다.

프레즌스 스팸이란 프레즌스 이벤트 패키지를 위한 Subscribe 요청 헤더를 사용하여 사용자 메신저 시스템의 친구 목록 혹은 화이트 목록(white list)에 등록될 수 있도록 시도한다. 혹은 고의적으로 Subscribe 요청 메시지를 발생시킬 때, 광고를 위한 주소를 사용한다면 이것 자체가 Spam 성격을 갖는다. 사용자는 이러한 Spammer의 프레즌스 요청을 자주 수신하게 되면 불편을 느낄 수 있다

1.2 VoIP Spam 차단 기술

E-MAIL Spam이나 VoIP Spam이 많은 사람들의 불편을 초래함에 따라 이를 차단하는 여러 가지 방법이 연구 됐고 일부는 상업적으로 적용됐다. 일반적으로 사용되는 Spam 차단 방법들을 살펴보면 다음과 같다[3,4].

- 콘텐츠 필터링(Contents Filtering)
- 블랙/화이트 리스트(Black/White List)
- 동의 기반 통신(Consent based Communication)
- 콜 행위 패턴 조사
- 레퓨테이션 시스템
- Turing test

콘텐츠 필터링은 가장 널리 적용된 E-mail 스팸 차단 방법 중의 하나다. 이 방법은 수신된 E-mail의 내용을 검사하고 분석해 스팸으로 의심되는 메일들을 제거하는 것으로 베이시안 필터링이 이에 속한다. IM 스팸의 경우 이메일처럼 도착 후 검사가 가능하고 Plain Text 나 HTML/XML 기반이기 때문에 콘텐츠 필터링을 적용해 차단할 수 있다.

블랙/화이트 리스트는 스패머로 식별된 주소를 데이타베이스화해 송신자 주소에 대하여 필터링을 수행하는 방식이다. 하지만 업데이트 및 관리해야 하는 송신자 리스트가 점점 방대하게 늘어나므로 관리가 어려운 단점이 있다.

동의 기반 통신은 화이트리스트나 블랙 리스트와 연동해 사용된다. 만약, 사용자 A가 사용자 B의 블랙 리스트나 화이트 리스트에 등록되어 있지 않다면, A가 사용자 B와 대화하고 싶을 때, 사용자 A는 우선적으로 사용자 B에게 동의(Consent) 요청을 하게 된다. 이러한 동의 프레임워크(Consent Framework)는 현재도 프레즌스 서비스나 인스턴트 메시징 서비스에 적용되어 사용되고 있다.

콜 행위 패턴 조사는 서비스 제공자에 의해 제공되는 Anti-Spam Solution 이다. 서비스 제공자는 송신자가 보내는 콜의 내용, 송신자의 콜을 생성하는 주기, 횟수 및 행동 패턴 등을 분석하여 블랙 리스트와 화이트 리스트를 작성할 수 있다. Spammer가 아닌 정상 사용자는 초당 발생할 수 있는 콜의 수가 제한되어 있으므로 콜의 발생 빈도에 대한 스레시홀드(threshold), 총 발생량의 트래젝토리(trajectory)를 통해 우선적으로 의심되는 스패머를 판별하고 정밀한 행위 패턴 조사를 통해 블랙 리스트를 작성할 수 있다

레퓨테이션 시스템은 송신자마다 레퓨테이션 점수를 부여하는 방식으로, 블랙 리스트, 화이트 리스트와 연동해 사용된다. 레퓨테이션 시스템은 중앙 집중적인 메시지 통신 서비스에서 더 유용한데, 중앙 집중 서비스 방식에서 각사용자에게 레퓨테이션 개념을 도입해 각 사용자는 다른 사용자의 레퓨테이션을 피드백(Feedback)해 점수를 관리하는 것이다. 예를 들어, 스팸 발신자에게 수신자는 마이너스 점수의 레퓨테이션을 부여해 스팸 발신자를 블랙리스트에 올리게 된다.

1.3 Turing Test

Turing Test란 기계에 지능이 있는지 여부를 판별하기 위한 테스트 방법으로, Alan Turing이 1950년에 제안하였다[5]. 이 방법은 인터넷에서 CAPTCHA(Completely Automated Public Turing test to tell Computers and Humans Apart)로 발전하여 컴퓨터와 인간을 구별하는데 사용된다. 인간은 구별할 수 있지만 컴퓨터는 구별하기 힘들게 의도적으로 비틀어 놓은 그림이나 문자를 주고 그 내용의 답변을 요구함으로써 자동화된 기기의 접근을 제어한다(그림 1). Turing Test는 자동화된 기기를 이용한 Call Spam의 효과적인 차단기술이지만 정상적인 사용자에게 불편을 야기 시킨다는 점에서 단점을 가지고 있기에 VoIP Service의 부분적인 분야(Voice Mail)에서 사용되고 있다.

본 논문에서는 VoIP Spam 중 Call Spam 만을 고려한다. 기존의 ITSP가 제공하는 Anti-VoIP Call Spam Solution의 문제점과 Turing Test 적용의 문제점을 분석하고, 이를 해결하기 위한 Ticket Turing Test를 제안한다. 본 논문의 구성을 다음과 같다. 제2장에서는 ITSP가 제공하는 VoIP Call Spam Solution의 문제점과 Turing Test 적용의 문제점을 소개한다. 3장에서는 기존 ITSP가 제공하는 Anti-VoIP Call Spam Solution의 문제점을 해결하기 위한 새로운 Turing Test 기법을 설명하고 4장에서는 실험 및 토론을 5장에서는 결론 및 향후 연구 방향을 제시한다.

그림 1 Turing Test의 예

2. 기존 연구

2.1 ITSP의 VoIP Spam 차단 기술

ITSP 서비스 제공자는 하나의 방법이 아닌 다양한 방법을 사용하여 Anti-VoIP Spam을 처리 하고 있다. 인스턴트 메시징 스팸이나 프레즌스 스팸의 경우 ITSP에서 콘텐츠 필터링을 이용하여 광고가 들어간 신호를 차단함으로써 사용자의 Spam에 대한 불편을 줄일 수 있다[6].

하지만 Call Spam의 경우실시간 데이타를 분석하여 Spam 처리를 하기는 어려우며, 이미 녹음된 광고음성을 듣는 사용자에게는 큰 불편을 야기할 것이다. 이러한 Call Spam의 경우에는 콜 행위 패턴 조사를 통하여 Spam 방지를 할 수 있다. 송신자의 행위를 분석하여 Spammer 인지 분석 하는 방법은 오직 ITSP 서비스 제공자처럼 중앙화된 서버를 갖고 있을 경우에 이를 적용할 수 있다. 예를 들어 한국의 '삼성 와이즈넷'의 경우 IP 센트릭스 서버와 보이스 플로우라는 솔루션을 이용하여 Anti-VoIP Call Spam Solution을 제공하고 있다. 이는 하나의 번호에서 다양한 호의 발생을 막거나 초당 호의 수(20개)를 제한함으로써 VoIP Call Spam을 막고 있는 방법이다.

2.2 접근 방식

2.2.1 ITSP의 VoIP Spam 차단 기술의 문제점

수면 중의 VoIP Call Spam은 사용자에게 큰 불편을 야기하기에 완벽한 Anti-VoIP Call Spam Solution은 필요하다. 하지만 기존의 콜 행위 패턴 조사를 이용한 Spam 처리의 경우 이미 발생된 VoIP Spam을 근거로 하기에 Call Spam을 겪은 사용자 입장에서는 불편이 야기될 것이다. 또한 Spammer는 제한된 번호를 바꾸거나 정해진 초당 호의 수를 넘지 않는 Call을 발생시킴으로써 콜 행위 패턴 조사를 피해 갈 수 있다. 더구나 몇몇 ITSP는 사용자에게 발신만을 허용시키는 VoIP Service를 제공한다. 이러한 서비스는 모든 사용자가 발신 시 동일한 번호를 사용하기에 ITSP에서 콜 행위 패턴 조사를 적용하기 어렵다. 이러한 Service는 Spammer에게 좋은 표적이 될 것이다[7].

2.2.2 ITSP에서 Turing Test의 어려움

Turing Test는 자동화된 기기를 이용한 VoIP Call Spam을 막기 위한 좋은 Solution 임에도 불구하고 정상적인 사용자 또한 Turing Test로 인하여 불편을 겪는다는 단점을 지니고 있다. ITSP에 의한 Turing Test 적용의 방법은 다음과 같다[8,9].

- 모든 Call 요구 시 마다 송신자에게 Turing Test 요구
- 최초 Call 요구 시 송신자에게 Turing Test 요구, 통과 시 Valid time 설정
- 수신자에 근거하여 송신자에게 Turing Test 요구, 통과 시 수신자에 근거한 Valid time 설정

첫 번째 방법은 전화를 걸 때마다 사용자에게 Turing Test를 요구함으로써 정상적인 사용자에게 큰 불편을 야기할 것이다. 두 번째 방법은 이러한 불편을 줄이기 위해 송신자에게 최초 연결 시 Turing Test를 요구하고 통과 시 정해진 시간 동안 송신자의 모든 Call을 허용하는 것이다. 그러나 이러한 방법은 Valid time 취득 후 이용되는 악의적인 Spam을 허용하게 된다. 세 번째 방법은 VoIP Spam 의 특성을 고려한 방법이다. 이미 광고를 보낸 수신자에게는 광고 Spam을 다시 보내지 않는다는 특성을 고려한 수신자 근거 Turing Test 방법이다. 송신자에게 Turing Test를 요구하고 통과 시 정해진 시간 동안 수신자의 번호만 Turing Test를 통과하도록 하는 방법이다. 그러나 이 방법은 ITSP에서 관리해야 하는 데이타가 점점 방대하게 늘어나므로 ITSP에게 어려운 방법이 아닐 수 없다.

2.2.3 본 논문의 접근 방식

본 논문은 ITSP에서 적용하기 어려운 Turing Test를 사용자단에서 처리함으로써 Anti-VoIP Call Spam을 제안하고 있다. 제안된 방법에서는 송신자 별 Turing Test를 통해 VoIP Call Spam을 방지하고 Turing Test를 통과한 송신자에게 Valid Time Ticket을 부여함으로써 재발신시 Turing Test를 다시 거쳐야 하는 송신자의 불편을 줄인다. 기존에 ITSP에서는 방대한 데이타 때문에 어려웠던 관리 문제는 송신자단에서 관리함으로써 관리가 용이해 진다.

3. 제안된 방법

3.1 전체 구조

그림 2는 제안된 방법의 전체 구조를 나타낸다. 송신자는 ITSP를 거쳐 수신자의 IP-PBX에 접근한다. IP-PBX는 Turing Test를 통하여 정당한 송신자와 VoIP Spam을 구분할 수 있다.

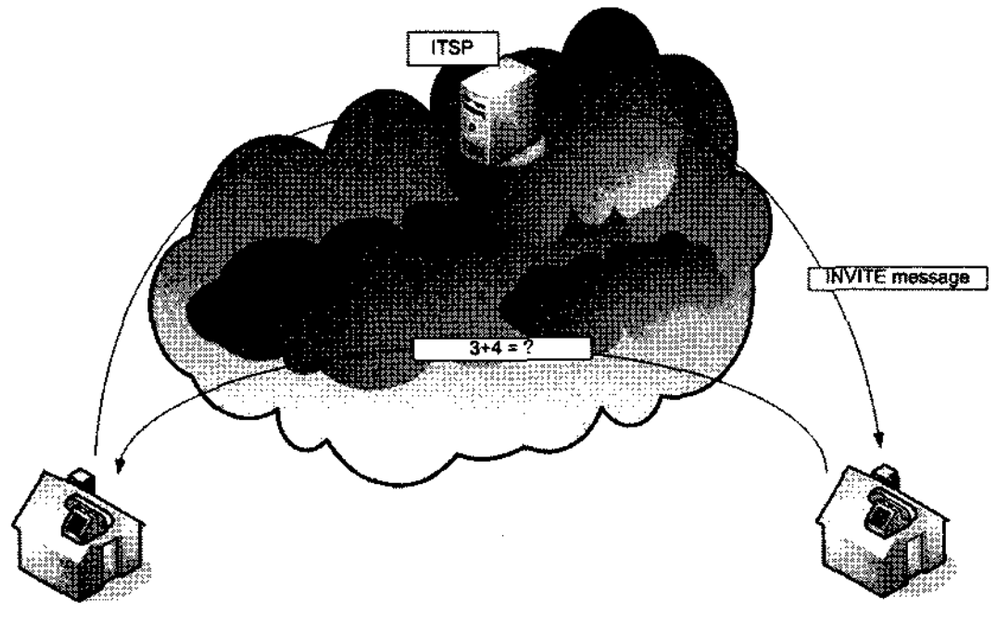

그림 2 제안된 방법의 전체구조

3.2 동작 과정

그림 3은 제안된 방법 Ticket Turing Test의 동작 과정을 나타낸다. 제안된 방법의 동작과정을 정리하면 다음과 같다

Step 1. 송신자의 SIP invite message는 전해진다. 이때 수신자의 white/black list를 체크하여 송신자를 구분한다. Black list에 걸러진 Spammer에게는 경고 음성을 전달 할 수 있다. 수신자 단에서의 white/black list 관리는 ITSP에 의한 white/black list 보다 송신자에게 근접하여 관리하기 용이하다는 장점이 있다.

Step 2. white/black list에 해당하지 않는 송신자는 Temporary list에서 확인한다. Temporary list는 Turing test를 통과한 송신자의 번호 및 valid time을 가짐으로써 재발 신을 하는 송신자가 추가적인 Turing Test를 거치는 불편을 줄일 수 있다.

Step 3. Temporary list에 없는 송신자나 valid time이 지난 송신자는 Turing test를 정해진 횟수 안에 응답함에 따라 valid ticket을 획득할 수 있다. Turing test의 정해진 횟수 혹은 시간을 초과한 Spammer는 black list에 추가됨으로써 연속적인 전화연결로 수신자의 전화를 방해하는 악의적인 행동을 방지 할 수 있다.

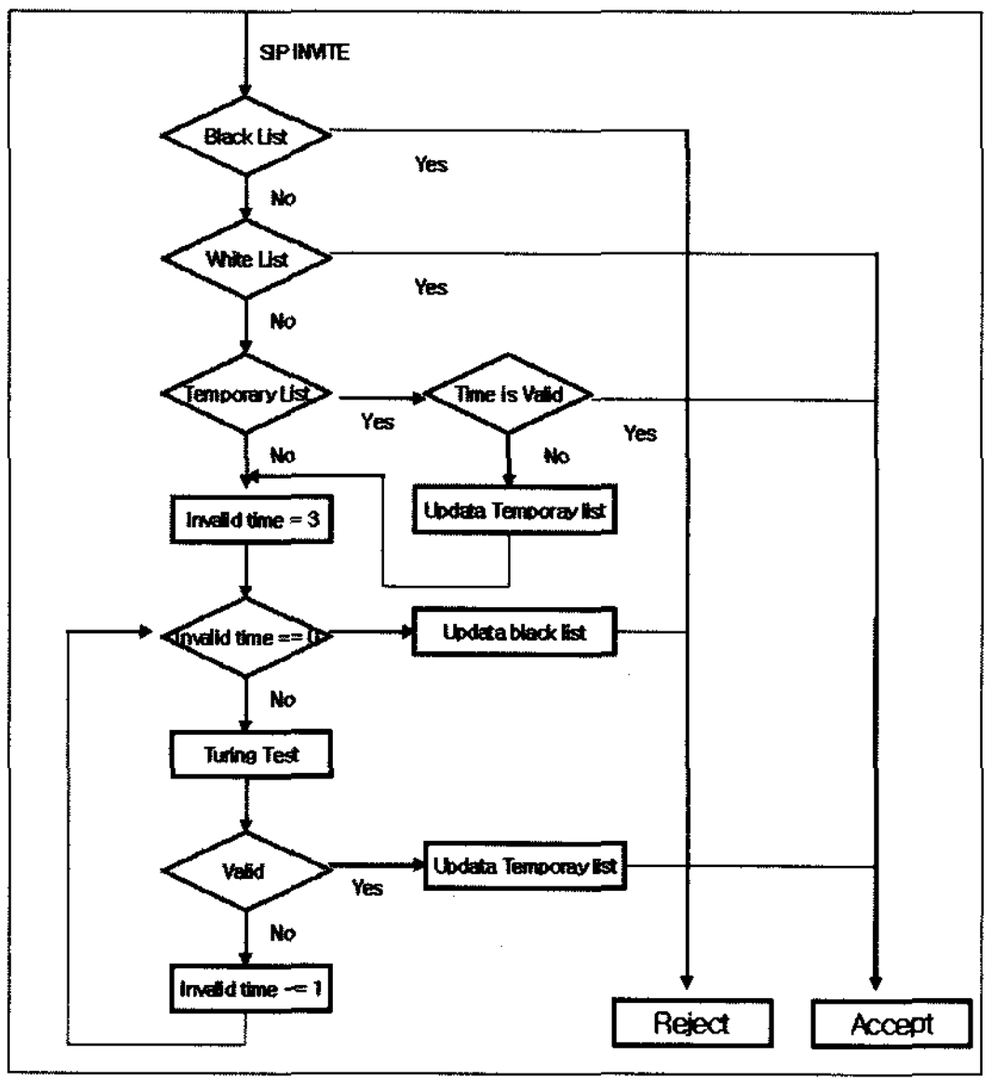

그림 3 제안된 방법의 동작과정

4. 실험 및 토론

4.1 실험 환경

실험의 전체적인 구성은 그림 4와 같다.

실험 구성에 사용된 하드웨어 소프트웨어를 정리하면

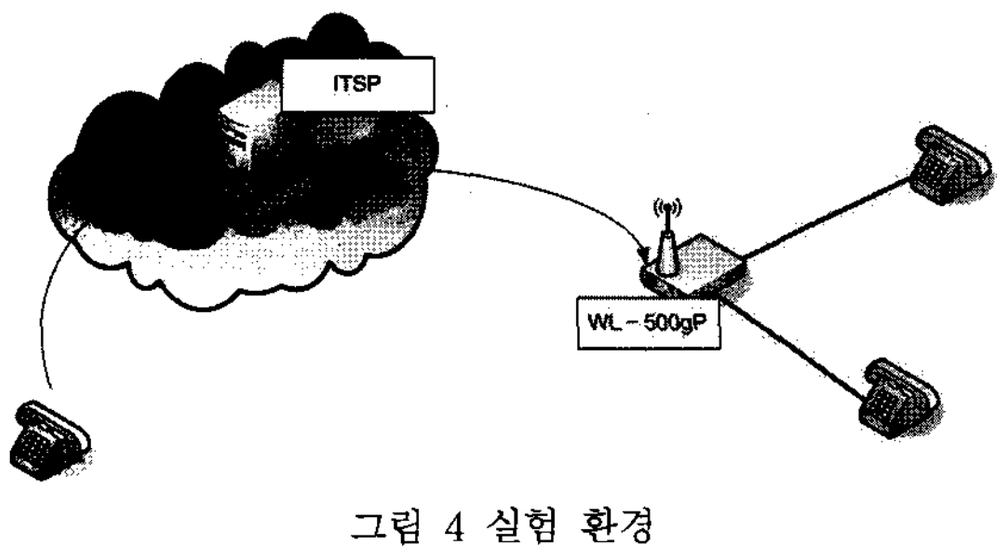

그림 4 실험 환경

표 1 실험에 사용된 하드웨어와 소프트웨어

하드웨어	ASUS WL-500G Premium 유무선 공유기 CPU : Broadcom 4704 266MHz RAM : 32 MB
운영 체제	OpenWRT (Linux Kernel 2.4)
소프트웨어	OpenPBX Asterisk 1.0

표 1과 같다. PBX는 집안 내 설치됨으로써 ITSP와 집안 내 전화기들 중간에 위치한다.

실험은 ASUS WL-500G Premium 제품상에서 OpenWRT 및 PBX software Asterisk를 설치하였다. 이때 운영체제는 Linux Kernel 2.4.30을 사용하였고, 제안된 방법은 Asterisk의 configure file을 수정하여 구현 하였다.

4.2 토 론

제안된 방법의 장점은 크게 2가지로 요약될 수 있다. 하나는 ITSP가 제공하는 Anti-VoIP Call Spam Solution의 불안전한 처리로 인한 VoIP Call Spam 발생 가능성을 가정 내 추가적인 Turing Test Solution을 통해 방지한다는 것이다. 나머지는 ITSP VoIP Service 뿐만 아니라 Peer to Peer VoIP Service의 사용 시 염려되는 VoIP Spam 또한 방지될 수 있다.

제안된 방법의 단점은 추가적인 하드웨어의 설치를 필요로 한다는 점이다. 하지만 본 실험의 구성처럼 추가적인 하드웨어 대신 가정 내 유무선 공유기에 PBX software를 이용함으로써 추가적인 하드웨어의 필요성은 사라진다. 또한 유무선 공유기에 설치된 PBX software는 가정 내 VoIP 기기의 유동적인 연결뿐만 아니라 사용자에게 ITSP service와 Peer to Peer Service의 동시 사용을 가능케 하며 Voice Mail과 같은 다양한 부가 서비스를 사용할 수 있게 한다.

5. 결 론

본 논문에서는 기존 ITSP가 제공하는 Anti-VoIP Call spam의 단점을 보완하는 사용자단 Turing Test에 대해 제안 하였다. 기존 ITSP가 Threshold 값에 의한 콜 행위 패턴 조사를 통해 불완전한 VoIP Call Spam을 처리

하였다면 제안된 방법에서는 사용자가 송신자에게 Turing Test를 요구함으로써 Call Spam을 처리하였다.

향후 연구 방향으로는 Peer To Peer VoIP Service에서의 VoIP Spam 처리에 관해 생각해 볼 수 있다. 단지 Turing Test를 통한 VoIP Spam의 방지뿐만 아니라 Reputation Solution을 Peer들 사이에 교환함으로써 ITSP Server가 없는 Peer To Peer 환경에서 VoIP Spam 처리 방식이다.

참 고 문 헌

[1] 조영철, "VoIP 보안의 향후 전망", Network Times, 2005.

[2] S. Park, J. Kim, and S. Kang, "Analysis of applicability of traditional spam regulations to VoIP spam," The 8th International Conference Advanced Communication Technology, pp. 1215-1217, 2006.

[3] 이재일, "VoIP 보안위협과 대응방안", 한국정보보호진흥원, 2007.

[4] Sipera System, "Sipera Enterprise VoIP Security Solution," White Paper, 2006.

[5] 정수환, "VoIP Spam and Security," Korea Internet Conference (KRnet), 2006.

[6] VQIPSA, "VoIP Security and Privacy Threat Taxonomy," White Paper, 2005.

[7] J. Rosenberg et al, "The Session Initiation Protocol (SIP) and Spam," Internet-Draft, 2004.

[8] H. Tschofenig et al, "Anti-SPIT : A Document Format for Expressing Anti-SPIT Authorization Policies," Internet-Draft, 2007.

[9] 추현우, "OECD Anti-Spam Toolkit 권장정책 및 대응방안", 한국정보보호진흥원, 2007.