논문번호 12-37B-08-03

한국통신학회논문지 '12-08 Vol.37B No.08
http://dx.doi.org/10.7840/kics.2012.37B.8.630

향상된 Multi Gray-Leveling을 통한 VoIP 스팸 탐지 기법

채 강 석◆, 정 수 환°

A Scheme of VoIP Spam Detection Using Improved Multi Gray-Leveling

Kangsuk Chae◆, Souhwan Jung°

요 약

본 논문은 VoIP 환경에서 Call 스팸 대응 방법으로 제안된 Multi Gray-Leveling 기법에서 존재하는 오류를 감소시킨 향상된 Multi Gray-Leveling 기법을 제안한다. 기존 Multi Gray-Leveling 기법은 두 개의 다른 시간 주기를 두고 송신자의 호 연결시간 간격을 체크하여 스팸 가능성을 판단함으로 공격자의 호 연결시간 간격 조절을 통한 탐지 회피 가능성을 제한하는 장점이 있으나, 긴 주기의 설정에 따라서 정상 사용자도 스패머로 오판하는 가능성이 존재한다. 본 논문에서는 이러한 오류를 방지하기 위해서 발신자의 행동 패턴뿐만 아니라 수신자의 행동 패턴까지 활용한 향상된 Multi Gray-Leveling 기법을 제안한다. 제안 기법은 사용자의 직접적인 개입이 필요하지 않고, VoIP 서비스 제공자 데이터베이스의 수신자 통화 정보를 이용하여 손쉽게 계산이 가능한 장점을 가지고 있기 때문에 실효성 있는 VoIP 스팸 탐지 방법으로 활용될 수 있다.

Key Words : VoIP, Spam, Spam Detection, Multi Gray-Leveling, Call Duration

ABSTRACT

In this paper, we propose an improved Multi Gray-Leveling scheme which reduces the problems of the existing Multi Gray-Leveling scheme suggested as a way of prevention against call spam in VoIP environment. The existing scheme having two different time period distinguishes the possibility of call spam by checking the call interval, so that it prevents the spammer's avoidance controlling the call interval. This is the strength of the existing one but it can misunderstand the normal user as a spammer due to taking long term time period. To solve this problem, this paper proposes the upgrade scheme which utilizes the receiver's action pattern as well as the caller's action pattern. It has such a good strength that can do gray leveling via the collected information in the database of VoIP service provider without user's direct involvement. Hence it can be a very effective way of VoIP spam detection.

Ⅰ. 서 론

최근 스마트폰의 보급과 함께 인터넷을 이용한 간편한 음성 통화를 지원하는 VoIP 서비스가 확산되고 있다. VoIP를 이용한 통신은 PSTN (Public Switched Telephone Network) 또는 3G 무선통

※ 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2012-H301-12-4008)
◆ 주저자 : 숭실대학교 전자공학과, chaekhan@ssu.ac.kr, 정회원
° 교신저자 : 숭실대학교 정보통신전자공학부, souhwanj@ssu.ac.kr, 종신회원
논문번호 : KICS2011-12-632, 접수일자 : 2011년 12월 23일, 최종논문접수일자 : 2012년 8월 7일

신보다 통신비용이 저렴하기 때문에 스팸 공격에 활용되기 좋으며, VoIP 세션 설립을 위한 SIP (Session Initiation Protocol)[1]는 소프트웨어 기반의 자동적인 공격 도구의 개발이 간편하고 URI형태의 수신자 전화번호를 사용함으로 공격 대상의 수집이 용이하여 스팸 공격 위협에 쉽게 노출된다.

SIP 기반의 VoIP 환경에서의 스팸 공격의 유형은 크게 Call 스팸, IM (Instant Messaging) 스팸, Presence 스팸의 3가지로 분류할 수 있다[2]. Call 스팸은 SIP를 통한 양단간 세션 설립 후 미디어 채널을 통해 수신자에게 광고성 미디어를 전송하는 유형이다. IM 스팸은 이메일 스팸과 유사한 스팸으로서 스팸문구를 SIP 프로토콜을 통해 수신자에 전송하는 스팸 유형이다. Presence 스팸은 IM 스팸과 유사한 유형의 스팸으로서 버디 또는 화이트리스트 기능을 위한 subscribe 메시지에 광고성 문구를 넣어 전송하는 유형이다. IM 스팸과 Presence 스팸은 이메일 시스템에서의 컨텐츠 필터링과 같은 스팸 방어 기술을 활용하여 어느 정도 방어가 가능하지만, 미디어 세션의 연결 후에 음성 또는 영상을 보내는 Call 스팸은 연결 이전에 컨텐츠를 알 수 없고 음성 또는 영상 컨텐츠의 특성상 필터링 기법을 적용하기 어렵기 때문에 이메일 스팸 대응 기술을 그대로 활용하여 온전히 탐지하기가 어렵다. 따라서 Call 스팸을 사전에 방지하기 위해서는 기존 이메일 스팸 대응 기법을 VoIP 환경에 맞게 수정하거나 VoIP의 특성을 이용한 탐지 방법을 활용하여야 한다.

Call 스팸을 방어하기 위한 기법 중 기존 이메일 스팸 대응 기법을 활용한 방법으로는 화이트/블랙리스트 기법[2], Payment at risk 기법[2,3], Turing 테스트 기법[4] 등이 있으며, VoIP 특성을 이용한 스팸 대응 기법은 다중 호 연결 탐지, 호 연결 비율 탐지, SIP 오류 메시지 발생 비율 탐지 기법과 같은 모니터링 기법[5,6], 하나의 주기를 통한 모니터링 기법의 단점을 보완한 Multi Gray-Leveling 기법[7] 등이 있다. 이러한 Call 스팸 대응 기술 중에서 Multi Gray-Leveling 기법은 사용자 불편성이 없고, 두 가지 기준으로 스팸 여부를 판별하기 때문에 주기 조절을 통한 스팸 공격을 어렵게 하는 등 효과적으로 스팸 대응이 가능하다. 그러나 Multi Gray-Leveling 기법은 지속적인 호 연결이 필요한 정상 사용자에 대해서도 스팸으로 오판하는 긍정오류 발생 가능성을 가지고 있으며, 긍정오류가 발생한 후에 긍정오류 발생 가능성이 높아지는 단점을 가지고 있다.

본 논문에서는 Multi Gray-Leveling 기법의 오판 가능성을 줄이기 위해서 발신자의 행위 패턴뿐만 아니라 수신자의 행위 패턴까지 적용한 새로운 계산식을 제안한다. 제안하는 향상된 Multi Gray-Leveling 기법은 수신자의 통화시간 패턴을 활용하여 기존의 계산식의 가중치로 적용함으로써 오판 가능성을 줄일 수 있으며, 추가로 포함되는 가중치를 계산하기 위해서는 수신자의 평균 통화시간과 통화시간 표준편차만 이용하기 때문에 VoIP 서비스 제공자의 데이터베이스를 이용하여 쉽게 계산이 가능한 장점을 가진다.

본 논문의 구성은 다음과 같다. 2장에서 기존 Call 스팸 대응 기법에 대한 소개 및 문제점을 살펴보고, 3장에서는 제안 기법을 서술한다. 4장에서는 제안 기법에 대한 분석을 하고, 마지막으로 5장에서 결론을 맺으며 논문을 마무리 한다.

Ⅱ. 관련 연구

VoIP 환경에서 발생할 수 있는 스팸 유형 중 IM 스팸과 Presence 스팸은 미디어 세션이 설립되기 전에 SIP 메시지에 광고성 문구를 전송하는 스팸 유형이기 때문에 이메일 스팸 대응 기법을 거의 수정 없이 활용이 가능하다. 그러나 Call 스팸은 미디어 세션 설립 후 직접 음성을 전송하는 스팸이기 때문에 이메일 환경에서 사용되는 스팸 대응 기법을 그대로 사용하여 차단하기는 어렵다. 따라서 이메일 스팸 대응 기법을 VoIP 환경에 맞게 수정하거나 VoIP 환경의 고유한 특징을 반영한 새로운 스팸 대응 기법으로 발전시켜 적용시킬 필요가 있다. 본 장에서는 기존의 Call 스팸 방어를 위한 기법을 소개하고 문제점을 분석해 본다.

2.1. 리스팅 기법

이메일 환경에서 스팸 대응을 위한 대표적인 기술로는 블랙리스트/화이트리스트와 같은 리스팅 기법이 있다[2]. 이 기법은 Call 스팸 방어 기술로 그대로 활용이 가능하다. 블랙리스트은 스패머로 식별된 사용자 또는 수신자의 수신거부 목록을 데이터베이스로 구축한 리스트이고, 화이트리스트는 수신을 허용한 사용자의 목록을 데이터베이스로 구축한 리스트이다. 그러나 모든 사용자에 대해서 블랙리스트와 화이트리스트를 작성하기는 어려우며, 새롭게 생성되거나 처음 보는 전화번호에 대한 스패머인지 정상 사용자인지 판단할 기준이 없는 Introduction 문

제가 있다. 이러한 경우 블랙과 화이트의 중간인 Gray로 구분하고 별도의 공격 여부를 판단하는 기법을 적용하여 대응할 필요가 있다.

2.2. Payment at Risk 기법

Payment at risk 기법은 이메일 스팸 대응 기법을 VoIP 환경에 맞게 수정하여 적용한 방법이다[2][3]. 세션 설립 요청시 발신자는 일정 금액을 수신자에게 이체하고, 호 종료 후 수신자의 판단으로 스팸이 아닌 경우 금액을 환불 받는 방법이다. 그러나 이 기법의 경우 스팸이 아닌 경우라도 수신자가 악의적으로 환불을 거부할 수 있는 문제를 가지고 있고, 또한 사용자의 직접적인 개입이 필요한 불편함이 존재한다.

2.3. Turing 테스트 기법

이메일 스팸 대응 기법 중 하나인 Turing 테스트 기법은 일종의 문자를 그림으로 보여주고, 이 퀴즈를 풀 수 있는 사용자만 허용하여 자동화된 도구에 의한 대량 이메일 전송을 방어하는 기법이다. VoIP 환경에 맞게 수정하여 적용한 Turing 테스트 기법은 전화 통화에서 사용되는 통화 연결음을 challenge 값으로 이용하는 방법이다[4]. 세션 설립 완료 후에도 통화 연결음을 들려주면 정상 사용자는 기다렸다가 통화 연결음이 종료된 후 통화를 시작하지만, 자동화된 스팸 공격 도구라면 SIP의 세션 연결요청 수락 메시지를 확인하고 바로 음성 재생을 시작하는 특성을 이용하는 것이다. 그러나 이 기법은 세션 설립시 지연이 발생하는 사용자 불편성이 존재한다.

2.4. 모니터링 기법

모니터링 기법은 Proxy 서버를 경유하는 SIP 메시지 탐지와 같은 SIP 프로토콜의 특성을 이용한 스팸 탐지 기법이다. 대표적인 모니터링 기법으로는 다중 호 연결 탐지, 호 연결 비율 탐지, SIP 오류 메시지 발생 비율 탐지 등이 있다[5,6]. 다중 호 연결 탐지 기법은 발신자가 동시에 다중 세션을 설립할 경우 스패머로 판단하는 방법이다. 호 연결 비율 탐지 기법은 일정 주기를 두고 그 주기 동안 발신자의 세션 설립 수가 임계값 이상이 되면 스패머로 판단하는 방법이다. SIP 오류 메시지 발생 비율 탐지 기법은 발신자가 일정 주기 동안 임계값 이상의 SIP 오류 메시지를 수신할 경우 다수의 도메인 이름과 사용자 이름을 생성하여 연결을 시도하는 스패머로 판단하는 기법이다. 이러한 모니터링 기법은 주기를 계산하여 호 연결 횟수를 조절하는 방법으로 회피가 가능한 단점이 있다.

2.5. Multi Gray-Leveling 기법

Multi Gray-Leveling 기법은 일반적인 모니터링 기법의 취약성을 개선하기 위해 제안된 기법이다[7]. 이 기법은 일반적인 모니터링 기법이 가지고 있는 공격자가 호 발생 주기를 조절하여 회피가 가능한 문제를 해결하기 위해서 두 개의 모니터링 주기를 두고 Multi Gray-Leveling으로 스팸 가능성 점수를 계산하는 기법이다. 이 기법에서는 발신자가 화이트리스트와 블랙리스트에 속하지 않는 경우 스패머인지 탐지하기 위한 점수계산을 Gray-Leveling이라 명칭하고, 길이가 다른 두 개의 주기를 기반으로 다른 계산식을 사용하여 합산하는 방식을 Multi Gray-Leveling로 정의하였다. 이 기법에서 짧은 주기를 기반으로 하는 계산식은 빠르게 점수가 상승/하강 하고, 긴 주기를 기반으로 하는 계산식은 느리게 점수가 상승/하강 하며, 이렇게 계산된 두 개의 점수를 합산하여 임계값 이상이 되면 스패머로 판단하게 된다.

표 1은 기존 Multi Gray-Leveling 기법의 표기법을 나타내고, 그림 1은 의사코드를 나타낸다. 그림 1의 a 단계는 긴 시간주기 Gray-Leveling 계산식이고, b 단계는 짧은 시간주기 Gray-Leveling 계산식이다. 각 시간주기에 따른 계산 결과의 의미를 살펴보면, 짧은 시간주기 계산식은 짧은 시간에 많은 연결을 시도하는 것을 탐지하기 위함이고 긴 시간주기 계산식은 지속적이고 주

표 1. 표기법
Table 1. Notation.

표기	설명
L	긴 주기 Gray Level (스팸 점수)
S	짧은 주기 Gray Level (스팸 점수)
PL	이전 단계까지 계산된 긴 주기 Gray Level
PS	이전 단계까지 계산된 짧은 주기 Gray Level
TL1	짧은 기준 시간주기
TL2	긴 기준 시간주기
I	이전과 현재 통화의 호 발생 시간 간격
T	스팸 결정 임계값
C1	S 계산시 가중치 값
C2	L 계산시 가중치 값
SH	스팸 히스토리, 스팸으로 판정시 1씩 증가

a. 1. If TL2-I >0,

$$L = PL + (C2 \times (SH+1) \times \frac{TL2 - I}{TL2})$$

2. If TL2-I<=0,

$$L = PL + (C2 \times (1 - \frac{SH}{SH+1}) \times \frac{TL2 - I}{TL2})$$

3. If L<0, then set L to 0

b. 1. If L<T,

$$S = PS + (C1 \times \frac{TL1 - I}{\min(\max(I,1), TL1)})$$

2. If S<0, then set S to 0
3. If S>=T, let L=S and S=0

c. If PS+PL<T and S+L>T, then SH++

그림 1. 기존 Multi Gray-Leveling 의사코드
Fig. 1. The pseudo code of existing Multi Gray-Leveling.

기적으로 연결을 시도하는 것을 탐지하기 위함이다. 만약 공격자가 탐지를 회피하기 위해서 호 연결 횟수를 조절하는 경우 짧은 시간주기에 의한 판단은 어렵지만 긴 시간주기에 의해서 지속적으로 레벨(스팸 가능 점수)이 상승하여 결국 스팸 공격으로 탐지가 되는 방식이다.

이 기법은 기존의 하나의 주기만을 가지고 스패머를 판별하는 기법과 다르게 스패머가 지속적으로 호를 발생시키는 경우 긴 주기 계산식에 의해서 스팸 점수가 누적되도록 설계되어 있으며, 이 경우 스패머의 레벨링 점수는 결국에 임계값을 넘게 되기 때문에 스팸 차단을 용이하게 할 수 있는 장점을 가진다. 만약 스패머가 긴 주기까지 고려하여 스팸을 전송한다고 가정하더라도 짧은 시간에 대량으로 스팸 전송이 어렵기 때문에 이 기법은 효율적인 스팸 차단 효과를 가진다. 그러나 이 기법은 업무상 주기적으로 호를 발생시키는 특징을 가지는 정상 사용자까지 스패머로 오판하는 긍정오류 발생 가능성을 가지고 있으며, 한번 긍정오류가 발생한 경우 SH (스팸 히스토리)가 가중치로 적용되기 때문에 오판한 사용자에 대한 회복이 어려운 문제가 있다.

Ⅲ. 제안 기법

본 장에서는 기존 Multi Gray-Leveling 기법에서 발생 가능한 긍정오류 발생에 따른 문제를 해결하기 위해서 수신자의 통화시간 패턴 기반의 피드백을 가중치로 활용하는 새로운 계산식을 제안한다. 이때의 수신자 피드백은 사용자의 직접적인 개입이 없이 수집이 가능한 수신자의 통화시간을 활용함으로써 사용자 불편성이 없도록 고려하였다. 기존 Multi Gray-Leveling 기법에서 지속적인 호 연결을 발생시키는 사용자는 무조건 레벨이 상승하기 때문에 오판 가능성이 존재한다. 따라서 제안하는 기법은 수신자의 통화시간 피드백을 활용하여 스팸 여부를 구분하고, 이를 기존의 긴 주기 계산식에 가중치로 적용하여 레벨의 상승 폭을 조절함으로써 오판 가능성을 감소시키고자 한다. 본 논문에서 제안하는 기법의 Call 스팸 탐지를 위한 가정은 발신자 측면과 수신자 측면의 행동 패턴에 대한 다음의 2가지이다.

- 스패머는 비교적 짧은 시간에 다량의 호 연결을 시도하고, 이러한 패턴은 지속적으로 이루어짐
- 수신자는 스팸 전화일 경우 짧은 통화시간을 가지고, 정상적인 전화일 경우 수신자의 평균 통화시간을 가짐

기존 Multi Gray-Leveling 기법은 위의 두 가지 조건 중 첫 번째만 고려하고 있기 때문에 정상 사용자에 대한 긍정오류가 발생하는 문제를 가진다. 긍정오류 문제의 해결을 위해 제안 기법에서는 두 번째 가정인 수신자의 통화시간 패턴을 고려한 기준을 계산식에 적용하여 정상적인 연결로 판단되는 호에 대해서는 레벨의 상승폭이 작아지도록 설계하였다. 제안 기법의 설계를 위한 기준 및 조건은 다음과 같다.

- 긴 기준 시간주기보다 발신자의 짧은 연결 간격, 수신자의 짧은 통화시간 피드백: 발신자가 스패머일 가능성 높음
- 긴 기준 시간주기보다 발신자의 짧은 연결 간격, 수신자의 긴 통화시간 피드백: 발신자가 스패머자일 가능성 낮음
- 긴 기준 시간주기보다 발신자의 긴 연결 간격: 스패머가 아닐 가능성이 높거나 스패머일 경우

표 2. 추가 표기법
Table 2. Additional notation.

표기	설명
F	수신자의 피드백 ($-1 \le F \le 1$)
D	현재 연결의 통화시간
Davr	수신자의 평균 통화시간
σ	수신자의 통화시간 표준편차
Z_t	수신자 통화시간의 표준정규분포 확률변수 제한값

a. 1. If TL2-I >0,

$$L = PL + (C2 \times (SH+1) \times \frac{TL2 - I}{TL2}) \times (\frac{1-F}{2})$$

2. If TL2-I<=0,

$$L = PL + (C2 \times (1 - \frac{SH}{SH+1}) \times \frac{TL2 - I}{TL2})$$

3. If L<0, then set L to 0

b. 1. If L<T,

$$S = PS + (C1 \times \frac{TL1 - I}{\min(\max(I,1), TL1)})$$

2. If S<0, then set S to 0
3. If S>=T, let L=S and S=0

c. If PS+PL<T and S+L>T, then SH++

그림 2. 향상된 Multi Gray-Leveling 의사코드
Fig. 2. The pseudo code of improved Multi Gray-Leveling.

라도 긴 주기에 따른 스팸 전송 제한이 성공적으로 수행된 것으로 판단

이러한 기준 및 조건을 바탕으로 새롭게 제안하는 계산식에 대한 추가적인 표기법은 표 2와 같고, 제안하는 계산식에 대한 의사코드는 그림 2와 같다.

제안하는 계산식은 긴 주기 Gray-Leveling 식에서 기준보다 짧은 통화 연결 간격을 가지는 경우 수신자의 통화시간 기반의 피드백 F를 가중치로 적용한다. 이때 수신자의 피드백 F는 -1에서 1 사이의 값을 가지며, 수신자 통화시간의 표준정규분포를 기반으로 계산된다. 수신자의 통화시간이 평균통화시간일 경우 피드백 F는 0이며, 평균통화시간을 기준으로 수신자의 통화시간이 짧을 경우 피드백 F는 -1에 가까워지고 길 경우 1에 가까워진다. 결과적으로 그림 2의 a단계 식 1은 수신자의 피드백 F에 따른 0에서 1사이의 가중치를 가지게 된다. 제안기법은 기존 기법에 비해 정상적인 호 연결에 대해서 레벨의 하강 폭은 동일하지만 상승 폭을 감소시키기 때문에 긍정오류 발생 가능성을 감소시킬 수 있게 된다.

a. If $D - D_{avr} < 0$,

$$F = \frac{\max(\frac{D - D_{avr}}{\sigma}, -Z_t)}{Z_t}, \quad (-1 \le F < 0)$$

b. If $D - D_{avr} \ge 0$,

$$F = \frac{\min(\frac{D - D_{avr}}{\sigma}, Z_t)}{Z_t}, \quad (0 \le F \le 1)$$

그림 3. 수신자 피드백 계산식
Fig. 3. The calculation of receiver's feedback.

발신자가 정상적인 사용자인지 판단하기 위한 수신자 피드백의 계산식은 그림 3과 같다. 수신자 피드백은 각 수신자의 통화시간 패턴 및 분포가 다르기 때문에 수신자 통화시간 표준정규분포를 이용하여 계산한다. 이때 수신자 피드백은 표준정규분포의 확률변수 제한값 Z_t에 의해서 -1과 1 사이의 값을 가지게 된다. 표준정규분포 확률변수 제한값 Z_t는 수신자 피드백 값의 정규화를 위한 값으로서 일정 확률 이내의 수신자 통화시간 분포만 고려하고, 그 확률 이외의 표준정규분포 확률변수 값을 $-Z_t$와 Z_t로 일반화한다. 수신자 통화시간의 표준정규분포 확률변수 계산값이 $-Z_t$이하의 값은 $-Z_t$로, Z_t이상의 값은 Z_t로 제한한다. 만약 Z_t의 값을 2으로 설정할 경우 그림 4와 같이 제한값 범위 안의 수신자 통화시간 분포확률은 95.44%이고, 이 경우를 전체 경우로 일반화 하는 것이다.

Ⅳ. 분 석

기존 Multi Gray-Leveling 기법은 발신자와 수신자 간의 관계에 상관없이 지속적으로 호를 발생시키는 경우 무조건 레벨을 상승시키지만 제안하는 기법은 둘 간의 관계를 고려하여 수신자의 통화시간에 따른 피드백을 적용하여 상대적으로 레벨을 상승시킨다. 그림 5는 통화시간 피드백에 따른 제안 기법의 긴 주기 Gray-Level의 상승 그래프이다. 그림 5의 그래프는 긴 기준 시간주기 TL2는 3600초 (1시간), 호 발생 간격 I는 180초 (3분), C2는 1이고, 수신자의 피드백 F의 평균값이 각 {-1, -0.9,

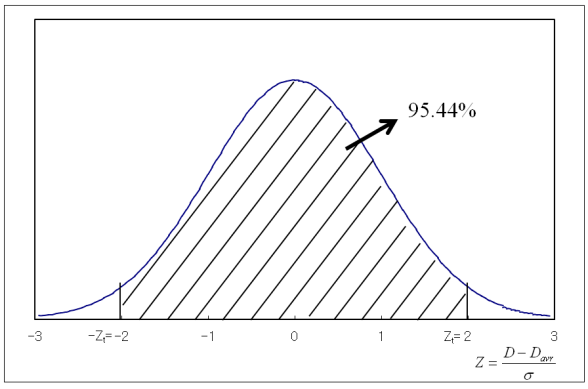


그림 4. 수신자의 통화시간 표준정규분포 그래프
Fig. 4. The standard normal deviate graph of receiver's call duration.

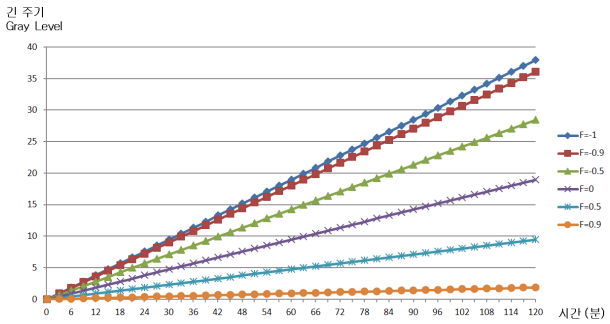


그림 5. 수신자 피드백에 따른 긴 주기 Gray Level
Fig. 5. Long-term gray levels according to receiver's feedback.

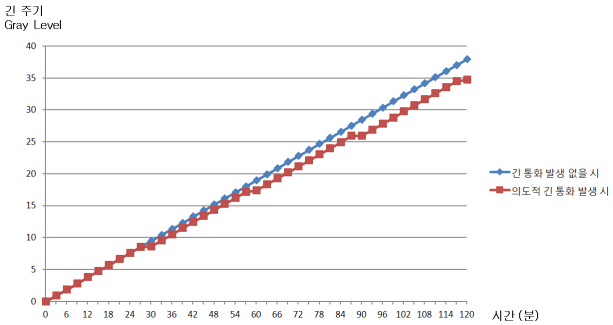


그림 6. 통화시간 조작에 따른 긴 주기 Gray Level
Fig. 6. Long-term gray levels according to manipulating call duration.

-0.5, 0, 0.5, 0.9}일 경우의 긴 주기 Gray-Level을 계산하여 표시하였다. 그림 5에서 수신자의 피드백이 -1일 경우는 기존 Multi Gray-Leveling 기법과 동일한 그래프를 가지며, 제안 기법에서의 의미는 수신자와의 통화시간이 매우 짧은 경우에 해당된다. 발신자가 매 3분마다 주기적으로 호를 발생시키더라도 수신자의 평균통화시간에 근접하거나 그 이상인 통화시간을 가지는 경우(F>0)는 긴 주기 Gray-Level의 상승 폭이 기존 Multi Gray-Leveling 기법(F=-1일 경우)에 비해 현저하게 낮은 것을 확인할 수 있다. 제안 기법에서는 이 경우를 수신자가 느끼는 발신자와의 통화가 충분히 유용한 상황으로 판단하여 스팸 가능성 점수를 적게 상승시키는 것이다.

제안 기법에서는 레벨 상승에 대한 가중치로 수신자의 통화시간 피드백을 적용하였으며, 이에 따른 사이드 효과로 스패머가 통화시간 조절을 통한 회피 가능성이 있는지 확인이 필요하다. 그림 6은 공격자가 일정 시간 주기 30분 단위로 충분히 긴 통화시간을 가지는 연결을 만들어낼 경우의 긴 주기 Gray-Level 그래프이다. 이때의 계산 파라미터는 그림 5의 계산 경우와 동일하고, 스팸 연결에 대한 수신자 피드백 F는 -1, 의도적 긴 통화시간을 가지는 경우의 수신자 피드백 F는 0.5에서 1사이로 랜덤하게 적용하였다.

그림 6에서 스패머는 일정 시간 주기인 30분 단위로 충분히 긴 통화시간을 가지는 연결을 만들어 내었고 10번의 호 연결 횟수 중 9회의 스팸을 발송하였다. 스패머가 발송한 10회 중 9번의 스팸에 대해서는 기존과 동일한 기울기로 긴 주기 Gray-Level이 상승하고, 긴 통화시간을 가진 경우만 작게 상승하는 것을 확인할 수 있다. 결과적으로 스팸을 발송한 횟수에 비해서 레벨 상승 폭은 동일한 것으로 확인할 수 있으며, 의도적 통화시간 조절을 통한 탐지 회피가 어려운 것을 알 수 있다.

V. 결 론

본 논문에서는 VoIP에서 발생 가능한 Call 스팸에 대한 대응 방법으로 기존 Multi Gray-Leveling 기법의 긍정오류 발생 가능성 문제를 개선시킨 기법을 제안하였다. 기존 기법은 발신자의 행동 패턴만 고려하여 계산식이 설계되었으나 제안 기법은 발신자의 행동 패턴뿐만 아니라 수신자의 행동 패턴까지 고려하여 계산식을 설계하여 더욱 정밀하게 스팸 가능성을 판별할 수 있는 장점을 가진다. 또한 수신자의 행동 패턴은 사용자의 직적접인 개입이 없이 VoIP 서비스 제공자의 데이터베이스에 저장된 정보를 이용하여 손쉽게 계산이 가능하기 때문에 실제 환경에 적용 및 활용이 용이하다는 장점을 가진다. 향후 연구방향으로는 VoIP 통화 시의 데이터를 수집하여 수신자의 통화시간 분포를 조사하고 실제 텔레마케팅과 같은 스팸 발송자의 호 발생 패턴을 분석하여 제안 계산식의 실효성을 검증하고 조금 더 정밀한 계산식을 설계하는 연구가 진행되어야 할 필요가 있을 것으로 생각된다.

References

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, SIP: Session Initiation Protocol, IETF RFC 3261, June 2002.

[2] J. Rosenberg, and C. Jennings, The Session Initiation Protocol (SIP) and Spam, IETF

RFC 5039, January 2008.

[3] M. Abadi, A. Birrell, M. Burrows, F. Dabek, and T. Wobber, "Bankable Postage for Network Services," *in Proc. of ASIAN '2003*, December 2003.

[4] J. Quittek, S. Niccolini, S. Tartarelli, M. Stiemerling, M. Brunner, and T. Ewald, "Detecting SPIT Calls by Checking Human Communication Patterns," *in Proc. of ICC '07*, June 2007.

[5] R. Schlegel, S. Niccolini, S. Tartarelli, and M. Brunner, "SPam over Internet Telephony (SPIT) Prevention Framework," *in Proc. of IEEE GLOBECOM '06*, November 2006.

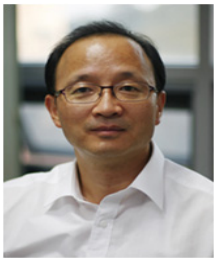
[6] B. Mathieu, S. Niccolini, and D. Sisalem, "SDRS: A Voice-over-IP Spam Detection and Reaction System," *IEEE Security and Privacy*, vol. 6, no. 6, pp. 52-59, November/December 2008.

[7] D. Shin, J. Ahn, and C. Shim, "Progressive Multi Gray-Leveling: A Voice Spam Protection Algorithm," *IEEE Network*, vol. 20, no. 5, pp. 18-24, September/October 2006.

채 강 석 (Kangsuk Chae)

2008년 2월 숭실대학교 정보통신전자공학부 학사
2010년 2월 숭실대학교 전자공학과 석사
2012년 3월~현재 숭실대학교 전자공학과 박사과정
<관심분야> 이동 네트워크 보안, VoIP 보안, SNS 보안, 클라우드 보안

정 수 환 (Souhwan Jung)



1985년 2월 서울대학교 전자공학과 학사
1987년 2월 서울대학교 전자공학과 석사
1988년~1991년 한국통신 전임연구원
1996년 6월 University of Washington 박사
1997년~1997년 Stellar One Corp. Senior Engineer
1997년~현재 숭실대학교 정보통신전자공학부 교수
<관심분야> 이동 네트워크 보안, VoIP 보안, SNS 보안, 클라우드 보안