논문 2013-50-2-18

SPIT 차단을 위한 예측 평판도 기법에 대한 연구

(A Study on Prediction Reputation System for Prevention of SPIT)

배 광 용*, 이 재 은*, 김 영 범**

(Kwang-Yong Bae, Jae-Eun Lee, and Young-Beom Kim)

요 약

본 논문에서는 실시간 동작 환경인 VoIP에 적용 가능한 스팸 대응 기법으로서 예측 평판도 시스템을 제안한다. VoIP 스템을 차단하기 위한 연구가 다양하게 진행되고 있지만, VoIP 스팸 대응을 위한 기존 기법들은 사용자의 직접적인 개입으로 인한 사용자 불편성, 실시간 동작으로 인한 세션 설립 시간 지연 및 시스템 과부하 등과 같은 문제가 있다. 제안 기법은 발신자의 세션 설립 주기와 수신자의 통화시간을 기준으로 통계적 방법을 이용하여 평판도를 계산하는 시스템이다. 제안 기법은 사용자의 직접적인 개입이 없기 때문에 사용자의 불편성 문제를 해결할 수 있으며, 실시간 동작을 요구하지 않고 세션 설립 전에 통계적 방법으로 발신자의 평판도를 계산하기 때문에 실시간 동작 환경인 VoIP에서 효과적으로 SPIT에 대응할 수 있다.

Abstract

This paper proposes a prediction reputation system for the anti-SPIT solution in real-time VoIP environment. The existing schemes need to get the user's feedback and/or have experienced the time delay and overload as session initiates due to real-time operation. To solve these problems, the proposed scheme predicts the reputation through the statistical analysis based on the period of session initiation of each caller and the call duration of each receiver. As per the second mentioned problem, this scheme performs the prediction before session initiation, therefore, it's proper for real-time VoIP environment.

I. 서 론

최근 VoIP 기술의 발전으로 이에 대한 서비스는 상용화되어 활발히 상품화 되면서 VoIP 스팸 문제가 중요한 이슈가 되고 있다. 특히 SIP 기반의 VoIP 환경에서 SIP는 텍스트 기반의 프로토콜로서 기존 이메일 시스템과 비슷한 스팸 공격이 가능하며, VoIP 환경은 PSTN 환경보다 비용이 저렴하기 때문에 쉽게 스팸 공격이 가능하다.

이런 이유로 VoIP 환경에서 스팸 공격에 대응하기 위한 방법들이 여러 방면에서 연구되고 있으며, 대부분의 기법들이 이메일에서 사용된 필터링 기법들을 재사용하고 있다. 이메일 스팸 대응 기법을 VoIP 환경에 맞게 적절히 수정한 기법으로 평판도 시스템 및 Payment at risk 기법[4], Turing 테스트 기법[5~6] 등이 있다. 그러나 이 기법들은 사용자의 직접적인 개입과 같은 사용자 불편성 문제가 존재한다. 또한 VoIP 환경에서 스팸은 세션 설립 완료 후 음성이나 영상을 전송하는 것과 같은 SPIT (Spam over IP Telephony)이 존재하기 때문에 이메일에서 사용되던 스팸 대응 기법만으로는 스팸 공격에 대한 완벽한 대응이 될 수 없다. 이러한 이유로 VoIP 환경의 특징을 이용한 Simultaneous calls, Call rate, Number of error messages associated with the caller, Progressive Multi Gray-Leveling (PMG) 등

* 정회원, KT G&E부문 PS본부 (KT)
** 정회원, 건국대학교 전자공학부 (Kunkuk University)
접수일자: 2012년11월27일, 수정완료일: 2013년1월15일

과 같이 사용자의 행동 패턴을 분석하는 새로운 SPIT 대응 기법이 제안되었다[2~3, 7]. 그러나 이 기법들은 사용자간 세션 설립 과정을 실시간으로 모니터링하고 동작하기 때문에 세션 설립 시간 지연이 발생하고 시스템 과부하가 존재하는 문제가 있다.

본 논문에서는 사용자의 직접적인 개입이 없고 실시간 동작 환경에 적용 가능한 예측 평판도 시스템을 SPIT 대응 기법으로 제안한다. 제안 기법인 예측 평판도 시스템은 발신자의 세션 설립 주기와 수신자의 통화 시간 기준의 피드백을 통계적 방법으로 분석하여 평판도를 계산하는 시스템이다. 따라서 제안 기법은 평판도 계산에 필요한 사용자의 직접적인 개입이 없기 때문에 사용자의 불편성 문제를 해결할 수 있으며, 세션 설립 과정 이전에 통계적 방법으로 평판도를 계산하기 때문에 실시간 동작으로 인한 세션 설립 시간 지연과 시스템 과부하가 작다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 SPIT 대응을 위한 관련 연구들을 살펴보고, Ⅲ장에서는 SPIT 대응을 위한 기법으로 예측 평판도 시스템을 제안한다. Ⅳ장에서는 예측 평판도 시스템의 적용 및 분석을 하고, 마지막으로 Ⅴ장에서 연구에 대한 결론을 맺는다.

Ⅱ. 관련 연구

VoIP 환경에서 발생할 수 있는 스팸 공격들은 크게 SPIT (Call 스팸), 인스턴트 메시징 (Instant Messaging, IM) 스팸, 프리젠스 스팸 등으로 나누어진다[1]. IM 스팸과 프리젠스 스팸은 세션이 설립되기 전 발생하는 스팸이기 때문에 이메일 스팸 대응 기법의 활용이 가능하다. 그러나 PSTN 환경에서의 텔레마케팅과 같은 SPIT은 세션 설립 후 직접 음성을 전송하는 스팸이기 때문에 이메일 환경에서 사용되던 스팸 대응 기법을 그대로 사용하여 차단하기에는 무리가 있다. 따라서 이메일 스팸 대응 기법을 VoIP 환경에 맞게 수정할 필요가 있다. 이러한 SPIT 대응 기법들은 어느 하나의 기법만으로 모든 SPIT에 대하여 완벽하게 대응하기 어렵기 때문에 다양한 기법들을 적절하게 배치하는 프레임워크가 필요하다. 본 장에서는 먼저 기존의 SPIT 대응을 위한 프레임워크에 대한 연구를 살펴본 후 프레임워크에 적용 가능한 기존의 다양한 기법에 대한 연구를 살펴본다.

2.1. SPIT 대응 프레임워크에 대한 연구

IETF RFC 5039 표준에서는 화이트리스트에 중점을 둔 프레임워크를 구성하는 방법을 제시하고 있다[1]. 이 표준에서는 SPIT 대응 프레임워크를 구성하기 위한 권장사항으로 강한 사용자 인증, 화이트리스트, 화이트리스트로의 사용자 추가 문제의 3가지 사항을 제시해주고 있다. 첫 번째 권장사항인 강한 사용자 인증은 화이트리스트와 블랙리스트와 같은 리스트 기법을 적용하기 위해서 필요한 조건이다. 만약 강한 사용자 인증이 적용되지 않은 VoIP 환경이라면 스팸 공격자는 다른 사용자로 위장하여 공격이 가능하기 때문에 리스트 기법의 효과가 감소할 수 있다. 두 번째 권장사항인 화이트리스트는 SPIT 대응 프레임워크를 구성하기 위한 핵심 기술로 스팸 공격자가 아닌 사용자의 지속적인 추가가 가능한 화이트리스트 기법을 사용하라는 것이다. 화이트리스트에 포함된 사용자는 다른 SPIT 대응 기법을 통하지 않고 빠르게 세션 설립 요청을 수락할 수 있기 때문에 화이트리스트를 적극적으로 사용하기를 권장하고 있다. 세 번째 권장사항인 화이트리스트로의 사용자 추가 문제는 스팸 공격자가 아닌 공격자를 어떻게 판단하여 화이트리스트에 추가할 수 있는지에 대한 방법을 제시하고 있다. 화이트리스트로의 사용자 추가 문제에 대한 방법으로 하나 이상의 SPIT 대응 기법을 적절하게 조합해서 스팸 공격자의 여부를 판단할 것을 권장하고 있다. 이러한 하나 이상의 SPIT 대응 기법을 구성하는 방법은 이미 알려진 여러 프레임워크 중 하나를 활용할 수 있고, 프레임워크에 적용 가능한 SPIT 대응 기법으로는 이메일 스팸 차단 기법을 응용한 방법 또는 SPIT 특징을 분석하여 새롭게 정의된 방법 등이 있다.

R. Schlegel 등은 SPIT 대응을 위한 프레임워크로 두 단계의 구조를 가지고 동작하는 프레임워크를 제안하였다[2]. 첫 번째 단계는 사용자의 개입 없이 스팸을 판단하는 단계이고, 두 번째 단계는 사용자의 직접적인 개입으로 스팸을 판단하는 단계이다. 첫 번째 단계에서는 사용자의 개입 없이 스팸을 판단하는 여러 기법들을 병렬로 배치하고, 각 기법의 결과를 합산하여 상향 임계값보다 크면 스팸으로 판단한다. 각 기법의 결과 값은 스팸으로 판단되면 1의 값을 가지고, 그렇지 않은 경우에는 -1의 값을 가진다. 이러한 각 기법 결과 값의 합이 상향 임계값보다 크면 스팸으로 판단하여 세션 연결 요청을 거절하고, 하향 임계값보다 작으면 스팸이

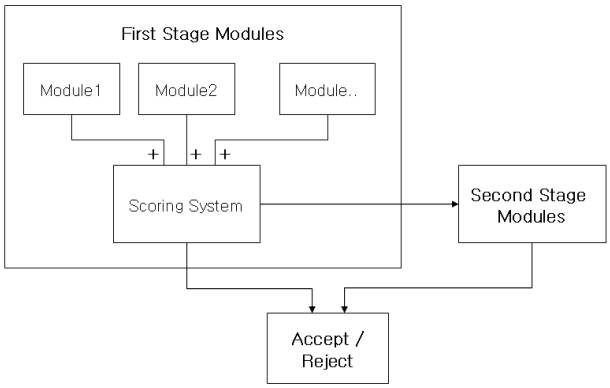

그림 1. 두 단계 구조를 갖는 SPIT 대응 프레임워크[2]
Fig. 1. SPIT prevention framework with two-step architectures[2].

아닌 것으로 판단하여 세션 연결 요청을 허락한다. 만약 각 기법 결과 값의 합이 상향 임계값과 하향 임계값 사이의 값을 가지면 스팸 여부의 판단을 할 수 없는 경우이기 때문에 두 번째 단계를 수행한다. 두 번째 단계에서는 사용자의 직접적인 개입이 필요한 Turing 테스트 같은 기법으로 스팸을 판단한다. 이와 같이 R. Schlegel 등이 제안한 프레임워크는 필요한 경우에만 사용자의 직접적인 개입이 요구되기 때문에 사용자의 불편성을 최소화하고 있으며, 첫 번째 단계에서 각 기법의 결과 값을 합산하는 방식을 사용하고 있기 때문에 새로운 스팸 대응 기법의 추가 및 제거가 용이한 장점을 가지고 있다.

B. Mathieu 등은 그림 2와 같이 사용자 구분 시스템, SPIT 검출 시스템, SPIT에 대한 반응 시스템을 주요 구성 요소로 가지는 SDRS (Spam Detection and Reaction System)을 제안하였다[3]. 사용자 구분 시스템은 사용자들의 피드백을 받아 사용자들의 행동 패턴을 수집하는 일종의 데이터베이스 시스템이다. 사용자들의 행동 패턴의 수집은 새롭게 블랙리스트에 추가되는 사용자를 포함하는 피드백과 같은 수신자 반응 또는 SPIT 검출 시스템에서 계산되어지는 발신자의 SPIT Level, 발신자의 호 설립 내력 등을 통하여 이루어질 수 있다. 또한 사용자 구분 시스템은 사용자의 행동 패턴을 분석하여 행동이 달라진 사용자를 검출하는데 유용하다. 정상적인 행동 패턴을 보이던 사용자가 갑자기 SPIT 발신자와 같은 행동을 보인다면, 이러한 사용자는 바이러스 또는 악성코드와 같은 해킹 공격을 당하는 것으로 추측할 수 있다. SDRS의 두 번째 구성 요소인

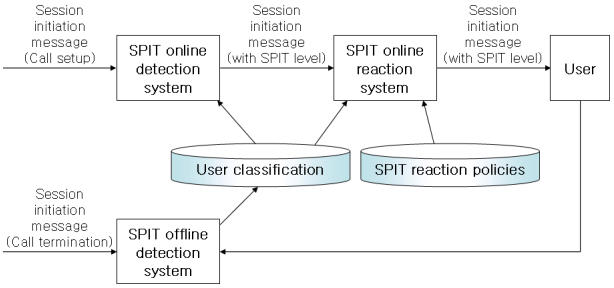

그림 2. SPIT Detection and Reaction System (SDRS)[3]
Fig. 2. SPIT Detection and Reaction System (SDRS)[3].

SPIT 검출 시스템은 다양한 스팸 대응 기법들의 점수를 통한 SPIT Level을 계산하는 시스템이다. 각 스팸 대응 기법들의 효율에 따라 가중치를 적용하고, 그 결과의 합으로 SPIT Level을 계산한다. SPIT 검출 시스템은 세션 연결 과정 중에 동작하는 SPIT 온라인 검출 시스템과 세션 연결 종료 후 동작하는 SPIT 오프라인 검출 시스템으로 이루어진다. SPIT 온라인 검출 시스템은 세션 연결 요청 메시지에 대한 모니터링 및 분석을 통한 기법들로 이루어지고, SPIT 오프라인 검출 시스템은 세션 연결 종료 후 사용자로부터 피드백을 받아 동작하는 기법들로 이루어진다. 마지막으로 세 번째 구성 요소인 SPIT에 대한 반응 시스템은 사용자 구분 시스템의 결과와 SPIT 검출 시스템의 SPIT Level에 따라서 어떻게 정책을 적용하여 반응할 것인지 결정하는 시스템이다. 여기에서 가능한 반응으로는 일정 주기 동안 연결 가능 세션 수의 제한, 임시 블랙리스팅, 수신자에게 통보와 같은 방법이 있다.

2.2. SPIT 대응 기법에 대한 연구

SPIT 대응 프레임워크에 적용 가능한 기법으로는 이메일 환경에서의 스팸 대응 방법을 응용하여 VoIP 환경에 맞게 수정한 방법과 VoIP의 특성을 이용한 새로운 스팸 대응 방법으로 구분하여 볼 수 있다.

이메일에서의 스팸 차단 기법을 VoIP 환경에 맞게 수정하여 적용하는 방법으로 평판도 시스템 및 Payment at risk 방법을 이용한 기법이 Y. Rebahi 등에 의해 제안되었다[4]. 이 기법은 사용자가 자신이 가지고 있는 전화번호 목록의 지인들을 직접 평가한 평점 정보를 기반으로 평판도를 계산하여 임계값 이하의 평판도를 갖는 SPIT을 차단하는 방법이다. 또한 Payment at risk 방법을 이용하여 SPIT 공격을 어렵게 한다.

Payment at risk 기법은 세션 설립 요청시 발신자는 일정한 금액을 수신자에게 이체하고, 세션 종료 후 수신자의 판단으로 SPIT이 아닌 경우 금액을 환불 받는 방법이다. 그러나 평판도 시스템은 평점을 계산하기 위해서 사용자가 직접 다른 사용자를 평가해야 하고 Payment at risk 기법은 금액의 과금 및 환불 여부를 확인하는 등의 사용자 불편성이 존재하며, 특히 Payment at risk 방법에서는 세션 설립시 발신자의 과금 확인 과정으로 인한 세션 설립 시간 지연 문제를 가지고 있다.

VoIP에서 Turing 테스트를 이용하여 발신자의 자동화 기계에 의한 스팸 전송 유무를 판단하는 방법이 J. Quittek 등에 의해 제안되었다[5~6]. 이 방법은 전화 통화에서 사용되는 링음을 Turing 테스트의 challenge 값으로 이용한다. 프락시 서버 또는 수신자 단말은 통화 연결이 완료된 후에도 링음을 전송한다. 정상적인 발신자라면 연결 설정이 완료되지 않은 것으로 판단하여 음성 전송을 시작하지 않고 대기하지만, 자동화 기계에 의한 SPIT 전송 도구이면 세션 연결 요청을 수락하는 SIP 메시지를 통하여 연결 설정이 완료되었음을 판단하고 즉시 SPIT 전송을 시작한다. 그러나 Turing 테스트 기법은 발신자의 테스트 과정을 거쳐야 하는 불편성이 존재할 수 있으며 테스트 시간으로 인한 세션 설립 시간 지연으로 인한 문제가 존재한다.

VoIP의 특성을 이용한 SPIT 대응 방법으로는 Simultaneous calls, Call rate, Number of error messages associated with the caller와 같은 모니터링을 통한 방법들이 있다[2~3]. Simultaneous calls 기법은 발신자가 동시에 멀티 세션을 설립할 경우 SPIT 발신자로 판단하는 방법이다. Call rate 기법은 일정 주기를 두고 그 주기 동안 발신자의 세션 설립의 수가 임계값 이상이 되면 스팸 발신자일 가능성이 크다고 판단하는 방법이다. Number of error messages associated with the caller 기법에서는 발신자가 일정 주기 동안 많은 수의 SIP 오류 메시지를 수신할 경우 다수의 도메인 이름과 사용자 이름을 생성하여 SPIT 공격을 하려는 발신자로 판단한다.

D. Shin 등은 위에서 살펴본 모니터링 기법들과 같이 하나의 주기만 가지고 있을 경우 세션 설립 주기의 조절을 통한 지속적인 SPIT 공격이 가능한 문제가 있기 때문에 두 개의 모니터링 주기를 두고 Leveling하는 Progressive Multi Gray-Leveling (PMG) 기법을 제안하였다[7]. PMG 기법에서는 짧은 주기와 긴 주기의 두 개의 주기를 두고 Gray-Leveling 한 후 그 두 점수를 합산한 값이 임계값을 넘으면 SPIT 발신자로 판단한다. 짧은 주기에 따른 Gray-leveling 점수는 빠르게 상승 또는 하강하고, 긴 주기에 따른 Gray-leveling 점수는 느리게 상승 또는 하강한다. 따라서 지속적인 주기로 세션 설립을 하는 SPIT 발신자라면 긴 주기에 따른 Gray-leveling에 의해 결국 임계값 이상이 되어 SPIT 발신자로 판단할 수 있다. 그러나 이 기법은 정상 사용자도 지속적인 세션 설립 주기를 가질 경우 PMG 점수가 임계값 이상이 되어 SPIT 발신자로 오판될 가능성이 존재하며, 매 세션 설립시 사용자 세션 설립 주기에 따른 레벨 점수의 계산을 수행하기 때문에 세션 설립 시간 지연과 세션 설립시 시스템에 과부하를 주는 문제도 존재한다.

Ⅲ. 예측 평판도 시스템

본 논문에서는 앞서 살펴보았던 기존 연구들의 문제점인 사용자 개입으로 인한 불편성 문제, 세션 설립 시간 지연 및 시스템 부하와 같은 문제를 고려하고 SPIT 대응 프레임워크에 적용 가능한 기법으로 예측 평판도 시스템을 제안한다. 예측 평판도의 적용을 위해서 SPIT의 특징 및 사용자의 반응을 다음과 같이 정의하였다. SPIT은 수신자가 원하지 않는 내용을 포함한 메시지를 사업적 관계를 갖지 않는 모든 사람이 보낸 모든 통신이다. SPIT 발신자는 비교적 짧은 시간에 대량으로 SPIT을 전송하는 행위를 한다. 수신자는 원하지 않는 내용을 포함하는 SPIT에 대한 세션을 빨리 종료한다. 자동화된 기계에 의한 SPIT 전송일 경우 일반적으로 사용자들의 평균 통화시간보다 짧은 시간의 SPIT 재생시간을 가진다.

예측 평판도는 사용자의 직접적인 개입이 들어가지 않는 피드백인 발신자의 세션 설립 주기와 수신자의 통화시간을 이용하여 통계적 방법으로 계산한 발신자의 평판도이다. 예측 평판도 시스템은 수신자의 통화시간 기준의 피드백 생성 동작과 발신자의 세션 설립 주기 및 수신자의 피드백 통계 동작, 발신자의 예측 평판도 계산 동작의 3가지 동작으로 이루어진다.

3.1. 수신자의 통화시간 기준의 피드백 생성 동작

수신자의 통화시간을 기준으로 피드백 레벨을 결정하기 위해서 그림 3과 같이 수신자의 통화시간 기반의 정규분포를 그린 후 통화시간이 짧은 하위 $\alpha\%$ 범위와 상위 $\alpha\%$의 범위, 그리고 상·하위 $\alpha\%$의 범위를 제외한 범위 (100-2$\alpha\%$) 의 3개의 범위로 나눈다. 그림 3에서 m은 수신자의 평균 통화시간을 의미하고, α는 스팸을 수신하였을 때 수신자의 반응을 조사하여 정할 수 있는 임의의 값이다. 발신자와의 통화시간에 따라서 다음과 같은 3가지의 피드백 레벨이 결정된다.

- F_1: 발신자와의 통화시간이 (m - b)보다 짧을 경우
- F_2: 발신자와의 통화시간이 (m - b)와 (m + b) 사이일 경우
- F_3: 발신자와의 통화시간이 (m + b)보다 길 경우

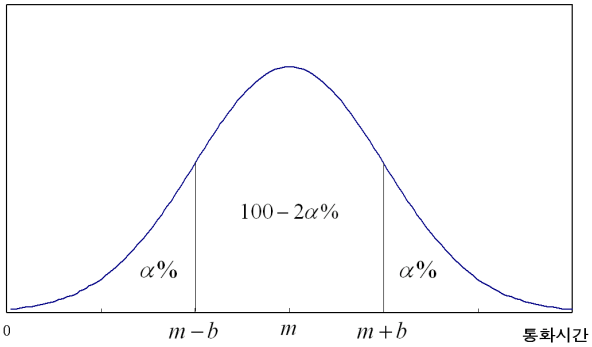

그림 3. 피드백 레벨 구분을 위한 수신자의 통화시간 정규분포 범위

Fig. 3. Normal distribution of recipient call duration for the feedback level classification.

3.2. 발신자의 세션설립주기 및 수신자의 피드백통계 동작

발신자의 세션 설립 주기의 통계를 구하기 위하여 T를 다음과 같이 정의한다. T는 스팸 여부 판단을 위한 이전 세션과 다음 세션의 설립 시간 간격으로 T보다 작은 세션 설립 주기를 가질 경우 스팸 발신자로 의심할 수 있는 임의의 기준 값이다. 발신자의 세션 설립 주기를 T와 비교하여 통계를 구하고, 발신자의 세션 설립 주기 전체 통계에 대한 r_1과 r_2의 비율을 다음과 같이 구한다.

- r_1: 발신자의 세션 설립 주기가 T보다 짧은 경우의 비율
- r_2: 발신자의 세션 설립 주기가 T보다 긴 경우의 비율

($r_1 + r_2 = 100\%$)

수신자의 각 피드백 레벨의 통계를 구한 후 발신자에 대한 수신자의 전체 피드백 중 d_1, d_2, d_3의 비율을 다음과 같이 구한다.

- d_1: 발신자에 대한 수신자의 전체 피드백 중 F1의 비율
- d_2: 발신자에 대한 수신자의 전체 피드백 중 F2의 비율
- d_3: 발신자에 대한 수신자의 전체 피드백 중 F3의 비율

($d_1 + d_2 + d_3 = 100\%$)

3.3. 발신자의 예측 평판도 계산 동작

발신자의 예측 평판도를 계산하기 위한 변수는 발신자의 세션 설립 주기 통계 값을 기준으로 계산된 R과 수신자의 피드백 레벨 통계 값을 기준으로 계산된 D가 있다. 발신자의 세션 설립 주기에 대한 비율과 수신자의 피드백 레벨에 대한 비율을 이용하여 R과 D를 구한 후 발신자의 예측 평판도인 P를 식 (1) ~ (3)과 같이 계산한다.

$$R = r_1 u + r_2 v \tag{1}$$

$$D = d_1 x + d_2 y + d_3 z \tag{2}$$

$$P = R \times D \tag{3}$$

u, v, x, y, z 값은 각 r_1, r_2, d_1, d_2, d_3에 대한 가중치이다. 각 가중치는 $u < v, x < y < z$ 또는 $u > v, x > y > z$ 조건이 되는 값을 가져야 한다. $u < v, x < y < z$ 조건의 가중치 값을 가질 경우 예측 평판도가 작을수록 스팸 발신자에 가깝다고 판단하고, $u > v, x > y > z$ 조건의 가중치 값을 가질 경우 예측 평판도가 클수록 스팸 발신자에 가깝다고 판단한다.

Ⅳ. 예측 평판도 시스템의 적용 및 분석

본 장에서는 제안 기법의 이해를 위해서 예측 평판도 시스템을 적용한 시뮬레이션 결과로 기본 동작을 확인하고 기존의 SPIT 대응 기법과 예측 평판도 시스템을 비교 및 분석한 결과를 살펴본다.

4.1. 제안 기법의 적용 및 동작 확인

제안 기법인 예측 평판도 시스템의 동작을 확인하고 이해하기 위해서 임의의 데이터 100개를 생성한 후 예측 평판도 시스템에 적용한 시뮬레이션을 수행하였다. 임의의 데이터를 기준으로 예측 평판도를 계산하고, SPIT 발신자로 판단할 수 있는 적정한 임계값을 도출하였다. 일반적으로 발신자의 세션 설립 주기가 짧고 수신자와의 통화시간이 짧을 경우 발신자의 예측 평판도가 작은 값을 가지도록 각 가중치의 값은 $u=0$, $v=1$, $x=0$, $y=0.5$, $z=1$과 같이 적용하였다. 각 가중치의 값을 예측 평판도 계산식에 적용하여 정리하면 식 (4)와 같다.

$$P = R \times D = 0.5 \times r_2 \times d_2 + r_2 \times d_3 \tag{4}$$

식 (5)를 이용하여 각 임의의 데이터의 예측 평판도를 계산한 후 각 데이터에서 발신자의 행동 패턴을 분석하기 위해서 SPIT 발신자와 정상 사용자를 구분하는 임계값을 450으로 정하였다. 각 데이터의 예측 평판도가 임계값인 450 이하일 경우 SPIT 발신자로 판단한다. 그림 4는 시뮬레이션의 결과로 각 데이터의 위상을 R과 D를 세로축 및 가로축으로 하는 그래프에 나타낸 것이다. 임계값 위상은 임계값을 450으로 하였을 때 나타나는 곡선으로 표현하였고, 그 식은 식 (5)과 같다.

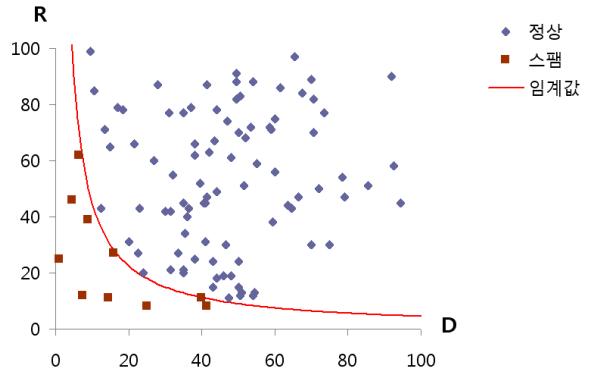

그림 4. 시뮬레이션 데이터 및 임계값의 위상 그래프
Fig. 4. Simulation data and phase graph of critical value.

$$R = \frac{450}{D} \tag{5}$$

표 1은 임의의 데이터 중에서 예측 평판도 시스템의 동작 확인을 위해서 사용자 행동 패턴별로 대표적인 값을 선택하여 정리한 것이다. 스팸 발신자로 판단된 데이터 9, 데이터 10의 사용자는 일반적으로 세션 설립 주기가 짧은 경우의 비율(r_1)이 높고, 수신자와의 통화시간이 짧은 경우의 비율(d_1)이 높다. 또한 데이터 7의 경우처럼 발신자의 세션 설립 주기가 긴 경우의 비율(r_2)이 높지만 수신자와의 통화시간이 짧은 경우의 비율(d_1)이 월등하게 높거나 데이터 8과 같이 발신자의 세션 설립 주기가 짧은 경우의 비율(r_1)이 수신자와의 통화시간이 짧지 않은 경우의 비율(d_2, d_3)보다 월등하게 높으면 SPIT 발신자로 판단한다. 데이터 1, 데이터 2와 같이 일반적으로 발신자의 세션 설립 주기가 길고(r_2), 수신자와의 통화시간이 길면(d_3) 정상 사용자로 판단한다. 데이터 3과 같이 전체적으로 비슷한 비율들을 갖는 사용자도 정상 사용자로 판단한다. 데이터 4, 데이터 5와 같이 일반적으로 짧은 통화시간을 갖는(d_1) 사용자라도 세션 설립 주기가 길면(r_2) 정상 사용자로 판단한다. 반면 짧은 세션 설립 주기를 갖는(r_1) 사용자라도 수신자와의 통화시간이 짧지 않다면(d_1) 데이터 6

표 1. 행동 패턴별 임의의 데이터 대푯값
Table 1. Random representative data for behavioral pattern.

구분	r_1	r_2	d_1	d_2	d_3	예측 평판도 P	스팸구분
데이터1	10	90	3	10	87	8280	정상
데이터2	16	84	22	21	57	5670	정상
데이터3	39	61	37	30	33	2928	정상
데이터4	34	66	76	19	5	957	정상
데이터5	15	85	82	15	3	892.5	정상
데이터6	81	19	22	60	18	912	정상
데이터7	38	62	91	5	4	403	스팸
데이터8	92	8	37	43	20	332	스팸
데이터9	73	27	73	22	5	432	스팸
데이터10	89	11	81	9	10	159.5	스팸

과 같이 정상 사용자로 판단한다.

위와 같이 사용자 행동 패턴에 따른 다음과 같은 결과를 얻을 수 있다. 일반적으로 세션 설립 주기와 통화시간이 짧은 사용자는 SPIT 발신자이다. 세션 주기가 긴 경우의 비율보다 통화시간이 짧은 경우의 비율이 월등이 높거나 세션 설립 주기가

짧은 경우의 비율이 통화시간이 짧지 않은 경우보다 월등히 높은 사용자도 SPIT 발신자로 판단한다. 반면 일반적으로 세션 설립 주기와 통화시간이 길거나 각 비율이 평균적인 분포를 보이는 사용자는 정상적인 사용자이다. 또한 일반적으로 통화시간이 짧아도 세션 설립 주기가 길거나 세션 설립 주기가 짧아도 통화시간이 짧지 않다면 정상 사용자로 판단한다.

4.2. 제안 기법 분석

- SPIT 오판 가능성 분석

SPIT 발신자를 정상 사용자로 잘못 판단하는 부정 오류는 기준 주기를 계산하여 SPIT 발신을 위한 세션 설립 주기를 조절하는 경우에 발생 가능하다. 그러나 이러한 SPIT 발신자라도 스팸 발신 주기를 조절해야 하기 때문에 제안 기법은 짧은 주기의 SPIT 전송을 막을 수 있는 효과가 있다. 반면 정상 사용자를 SPIT 발신자로 잘못 판단하는 긍정 오류는 주로 업무상 짧은 통화시간의 비율이 월등하게 높거나 짧은 세션 설립 시간 주기의 비율이 월등하게 높을 경우 발생한다. 이런 문제의 해결을 위해서 실제 데이터의 분석을 통한 예측 평판도 계산 공식의 변수와 임계값의 적절한 설정이 필요하다. 또한 SPIT 대응 프레임워크를 구성하여 다른 SPIT 기법과 병행 적용하는 것이 필요하다.

- 제안 기법의 동작 효율 분석

제안 기법은 사용자의 직접적인 개입이 들어가는 피드백이 아닌 사용자 행동 패턴에 대한 통계를 기준으로 평판도를 계산한다. 따라서 사용자의 개입으로 인한 사용자 불편성이 없다. 또한 실시간 동작에 있어서 세션 설립시 발신자의 예측 평판도와 임계값을 비교하는 연산 동작만을 수행함으로 세션 설립 시간 지연과 시스템 과부하가 작다.

4.3. 각 기법의 비교, 분석

본 절에서는 제안 기법의 효율성 분석을 위해 기존의 SPIT 대응 기법들이 가지고 있는 사용자 불편성, 실시간 동작에서 발생하는 문제점및 각 기법들의 SPIT 판단 기준을 비교해 보았다. 사용자 불편성은 사용자의 직접적인 개입이나 세션 설립 과정에서 사용자가 원하지 않는 대기시간과 같은 문제점이다. 실시간 동작에서 발생하는 문제는 각 기법의 적용을 위해서 발생할 수 있는 세션 설립 과정에서의 시간 지연과 세션 설립시 시스템 과부하 측면에서 분석하였다.

사용자 불편성 문제를 가지고 있는 기법은 기존의 평판도 시스템, Payment at risk 및 Turing 테스트 기법이다. 이 기법들은 이메일 환경에서의 스팸 대응 기법을 VoIP 환경에 맞게 수정하였으나 사용자 불편성과 같은 문제를 여전히 가지고 있다. 기존의 평판도 시스템은 각 사용자가 직접적으로 다른 사용자의 평가 점수를 평가해야 하는 불편성이 존재한다. Payment at risk 기법은 세션 설립 시의 과금 확인 과정에서 발신자의 개입이 필요하고, 세션 종료 시의 환불 확인 과정에서 수신자의 개입이 필요한 것과 같은 사용자 불편성을 가지고 있다. Turing 테스트 기법은 발신자가 테스트 과정을 수행해야 하는 것과 이미 세션 설립 요청에 응답한 수신자가 테스트 시간동안 기다려야 하는 것과 같은 사용자 불편성 문제를 가지고 있다.

각 기법의 실시간 동작에서 발생 가능한 문제를 분석하기 위해서 우선 SPIT 판단을 위한 동작이 주로 언제 수행되는지 비교한다. 기존의 평판도 시스템은 세션이 종료된 후 (오프라인) 사용자들이 직접 평가한 평점을 기반으로 평판도를 계산한다.

Payment at risk 기법은 과금 확인 과정이 세션 설립 요청시 동작하고, 환불 확인 과정이 세션 설립 종료시 동작한다 (온라인). Turing 테스트, Simultaneous calls, Call rate, Number of error messages associated with the caller, PMG 기법은 세션 설립 과정 중 (온라인) 동작을 수행한다. 예측 평판도 시스템은 기존의 평판도 시스템과 비슷하게 세션이 종료된 후 다음 세션 설립 과정이 수행되기 이전에 (오프라인) 예측 평판도의 계산이 이루어진다. 오프라인으로 동작하는 기존의 평판도 시스템과 예측 평판도 시스템은 세션 설립시 사용자 평판도와 임계값의 비교를 위한 지연 시간만 존재하여 실시간 동작으로 인한 시스템 과부하가 크지 않다. 온라인으로 동작하는 기법 중 Simultaneous calls, Call rate, Number of error messages associated with the

표 2. 기존 SPIT 대응 기법과 예측 평판도 시스템의 비교
Table 2. Comparison existing SPIT response techniques and prediction reputation system.

구분	기존의 평판도 시스템 [4]	Payment at risk [4]	Turing 테스트 [5][6]	Simultaneous calls [2][3]	Call rate [2][3]	Number of error messages associated with the caller [3]	PMG 기법 [7]	제안 기법
제안 유형	이메일 스팸 차단 기법의 수정			VoIP 특성에 따른 기법				
사용자 불편성	사용자의 직접적인 평점 평가	과금 및 환불 확인	발신자에 대한 테스트 과정 및 대기시간	-	-	-	-	-
기법 동작 시점	오프라인	온라인						오프라인
세션 설립 시간 지연	평판도와 임계값의 비교	발신자의 과금 확인 과정	발신자의 테스트 시간	주기 내 미종료 세션 수와 임계값의 비교	주기 내 세션 설립 횟수와 임계값의 비교	주기 내 오류 수신 횟수와 임계값의 비교	세션 설립 주기에 따른 점수계산, 임계값과 비교	예측 평판도와 임계값의 비교
실시간 동작으로 인한 시스템 과부하	-	과금을 위한 동작으로 인한 시스템 과부하	테스트 동작으로 인한 시스템 과부하	-	-	-	발신자의 레벨링 점수 계산으로 인한 시스템 과부하	-
SPIT 판단 기준	사용자의 직접적인 평점 피드백	수신자의 환불 과정 피드백	발신자의 테스트 통과 여부	멀티세션 수	세션 설립 주기	SIP 오류 메시지 수신 주기	세션 설립 주기	세션 설립 주기 및 통화시간

caller 기법도 SPIT 판단을 위한 값과 임계값의 비교를 위한 세션 설립 지연 시간만 존재하여 실시간 동작으로 인한 시스템 과부하가 크지 않다. 그러나 실시간 모니터링으로 인한 부담은 여전히 존재한다. 온라인으로 동작하는 다른 기법인 Payment at risk와 Turing 테스트, PMG 기법은 세션 설립 지연과 실시간 동작으로 인한 시스템 과부하가 크다. Payment at risk 기법은 세션 설립시 발신자에게 과금 확인을 위한 과정 때문에 세션 설립 지연 시간이 발생하고, 과금 과정에서 사용자 계좌로 일정한 금액의 이체 등과 같은 동작으로 인한 시스템 과부하가 크다. Turing 테스트는 발신자를 테스트하기 위한 시간으로 인해 세션 설립 지연 시간이 발생하고, 테스트를 위한 challenge 전송 및 응답 확인 동작으로 인한 시스템 과부하가 크다. PMG 기법은 사용자의 세션 설립 주기를 이용한 레벨링 계산 과정이 실시간으로 이루어져야 하기 때문에 시스템 과부하를 발생시킨다.

마지막으로 SPIT 판단 기준의 비교를 통하여 각 기법의 오판 발생 가능성을 분석해본다. 기존의 이메일 환경에서의 스팸 대응 기법을 수정하여 적용한 기법들은 사용자의 직접적인 개입이 들어가기 때문에 오판 발생 가능성이 크지 않다. 그러나 VoIP 특징을 이용한 새롭게 제안된 SPIT 대응 기법들은 사용자의 행동 패턴을 통한 SPIT 검출을 하기 때문에 오판 발생이 가능하다. 이러한 기법들은 대부분 SPIT 판단 기준을 사용자의 행동 패턴 중 어느 하나만 사용하기 때문에 그 행동 패턴을 피하는 경우 오판 가능성이 존재한다. 제안 기법은 SPIT 판단 기준으로 세션 설립 주기와 통화시간의 두 가지 사용자 행동 패턴을 사용하여 오판 가능성을 줄일 수 있다.

표 2는 기존의 SPIT 대응 기법과 제안 기법인 예측 평판도 시스템을 비교하여 정리한 것이다. 제안 기법은 사용자의 직접적인 개입이 들어가지 않는 피드백을 사용함으로 기존의 평판도 시스템이 가지고 있는 사용자 불편성 문제를 해결하였다. 또한 예측 평판도의 계산이 세션 설립 과정 이전에 동작함으로 세션 설립 지연 시간이 작고 실시간 모니터링 및 동작에 따른 시스템 과부하가 작다. 제안 기법은 기존 기법과 다르게 SPIT 판단 기준으로 사용자의 세션 설립 주기와 통화시간의 두 가지 사용자 행동 패턴을 사용하기 때문에 오판 발생률을 줄이는 것이 가능하다. 그러나 제안 기법도 대부분의 SPIT 대응 기법처럼 오판 가능성이 여전히 존재하

고 모든 SPIT의 완벽한 차단이 힘들기 때문에 다른 SPIT 대응 기법들과 병행 적용해서 SPIT 차단 효과를 높일 필요가 있다.

V. 결 론

본 논문에서는 실시간 동작 환경인 VoIP에서 적용 가능한 스팸 대응 기법으로서 예측 평판도 시스템을 제안하였다. 제안 기법은 발신자의 세션 설립 주기와 수신자의 통화시간을 기준으로 통계적 방법을 이용하여 평판도를 계산하는 시스템이다. 따라서 제안 기법은 사용자의 직접적인 개입이 없기 때문에 사용자의 불편성 문제를 해결할 수 있으며, 실시간 모니터링 동작을 하지 않고 세션 설립 과정 이전에 통계적 방법으로 발신자의 평판도를 계산하기 때문에 실시간 동작 환경인 VoIP에서 효과적으로 SPIT에 대응할 수 있다.

참 고 문 헌

[1] J. Rosenberg, and C. Jennings, The Session Initiation Protocol (SIP) and Spam, IETF RFC 5039, January 2008.
[2] R. Schlegel, S. Niccolini, S. Tartarelli, M. Brunner, “SPam over Internet Telephony (SPIT) Prevention Framework,” Proc. of IEEE GLOBECOM '06, November 2006.
[3] 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.
[4] Y. Rebahi, D. Sisalem and T. Magedanz, “SIP Spam Detection,” Proc. of IEEE ICDT '06, June 2006.
[5] J. Quittek, S. Niccolini, S. Tartarelli, and R. Schlegel, “Prevention of Spam over IP Telephony,” NEC Technical Journal, vol. 1, no. 2, pp. 114-119, February 2006.
[6] J. Quittek, S. Niccolini, S. Tartarelli, M. Stiemerling, M. Brunner, and T. Ewald, “Detecting SPIT Calls by Checking Human Communication Patterns,” proc. of ICC '07, June 2007.
[7] D. Shin, J. Ahn, C. Shim, “Progressive Multi Gray-Leveling: A Voice Spam Protection Algorithm,” IEEE Network, vol. 20, no. 5, pp. 18-24, September/October 2006.
[8] 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.

저 자 소 개

배 광 용(정회원)
2004년 건국대학교 전자정보통신공학과 박사수료
1990년 KT 연구개발본부 전임연구원
2002년~현재 KT G&E부문 부장
<주관심분야 : USN 보안, VoIP 보안, M2M통신>

이 재 은(정회원)
2009년 숭실대학교 컴퓨터학과 박사수료
2004년~현재 KT G&E부문 팀장
<주관심분야 : USN, M2M, 보안, Cloud, Multimedia, Big Data>

김 영 범(정회원)
건국대학교 전자공학부 교수
대한전자공학회논문지 제35권 S편 제4 참조