블룸필터를 사용한 화이트리스트 기반의 SIP 서비스 거부 공격 대응 기법

준회원 김 주 완*, 정회원 류 제 택**, 류 기 열*, 종신회원 노 병 희***°

A Countermeasure Scheme Based on Whitelist using Bloom Filter against SIP DDoS Attacks

Ju-Wan Kim* *Associate Member*, Jea-Tek Ryu** , Ki-Yeol Ryu* *Regular Members*,
Byeong-hee Roh***° *Lifelong Member*

요 약

SIP는 인터넷을 기반으로 하기에 기존 인터넷에서 발생하는 보안 위협에 노출되어 있어 서비스 거부 및 서비스 단절과 같은 문제를 야기하는 플러딩 공격에 영향을 받을 수 있다. 하지만 현재 제안된 서비스 거부 공격 대응 기법은 제안 기법의 복잡도와 다양한 서비스 거부 공격에 대응하지 못한다는 한계점이 있다. 그러므로 본 논문에서는 이러한 점을 고려하여 SIP 세션 설정 과정을 관찰하고 정상적인 세션을 맺은 사용자를 정상 사용자로 정의하여 이것을 이용한 화이트리스트를 구성함으로써 다양한 서비스 거부 공격 상황에서 정상 사용자에게 지속적인 서비스를 제공하고자 하는 방안을 제시한다. 본 방안은 다양한 공격 방법들을 네트워크 시뮬레이터인 OPNET을 이용하여 모델링하였고 서비스 거부 공격 시에도 지속적인 서비스 제공, 낮은 오탐율, 빠른 검색 시간을 달성코자 한다.

Key Words : SIP, DDoS, Bloom Filter, Whitelist, OPNET

ABSTRACT

SIP(Session Initiation Protocol) has some security vulnerability because it works on the Internet. Therefore, the proxy server can be affected by the flooding attack such as DoS and service interruption. However, traditional schemes to corresponding Denial of Service attacks have some limitation. These schemes have high complexity and cannot protect to the variety of Denial of Service attack. In this paper, we newly define the normal user who makes a normal session observed by verifier module. Our method provides continuous service to the normal users in the various situations of Denial of Service attack as constructing a whitelist using normal user information. Various types of attack/normal traffic are modeled by using OPNET simulator to verify our scheme. The simulation results show that our proposed scheme can prevent DoS attack and achieve a low false rate and fast searching time.

I. 서 론

VoIP (Voice over IP)는 인터넷의 다양한 멀티미디어 서비스를 쉽게 음성 통화 서비스와 통합하여 저렴하게 제공할 수 있다는 장점을 가지고 있다. 또한 IP (Internet Protocol)망을 이용하여 손쉽게

※ 본 연구는 지식경제부/정보통신산업진흥원의 대학 IT 연구센터 지원사업(NIPA-2011-C1090-1121-0011) 지원을 받아 수행되었음.
* 아주대학교 정보컴퓨터공학부 ({comomind, kryu}@ajou.kr), ** 한국특허정보원 (ryujeatek@hotmail.com)
*** 아주대학교 정보통신전문대학원 / 정보컴퓨터공학부 (bhroh@ajou.ac.kr), (° : 교신저자)
논문번호 : KICS2011-06-264, 접수일자 : 2011년 6월 20일, 최종논문접수일자 : 2011년 10월 28일

서비스를 제공할 수 있다는 점에서 기존의 PSTN (Public Switched Telephone Network)을 빠른 속도로 대체하고 있다.

VoIP에서의 시그널링과 세션 관리를 위하여 SIP (Session Initiation Protocol)가 많이 채택되어 사용되고 있다[9]. IETF (Internet Engineering Task Force)에서 제안한 SIP는 간단한 구조를 갖추어 개발과 구현이 용이하고 서비스의 확장성 및 포괄성이 뛰어나다. 또한 인터넷 망을 기준으로 설계되었기 때문에 기존 인터넷의 다양한 멀티미디어 서비스들이 쉽게 수용 가능한 장점이 있다. 따라서 대부분의 VoIP시스템은 SIP를 사용하여 시그널링과 세션 관리를 수행한다. 하지만 SIP는 HTTP와 유사한 텍스트 기반의 구조를 가지고 있고 개방형 네트워크를 기준으로 개발되었기 때문에 플러딩으로 인한 서비스 거부 공격과 같은 위협에 노출되어 있어 이에 대한 대응이 요구된다[1].

SIP의 보안 위협은 프로토콜의 취약점을 이용한 시그널링 공격과 다량의 SIP 메시지를 발생시켜 서비스 거부를 일으키는 플러딩 공격으로 구분된다[1]. 현재 시그널링 공격에 대한 대응 기법은 SIP 프로토콜 자체의 취약점을 보완하거나 메시지 암호화를 통해 많은 해결 방안과 연구가 진행되어 있다[2],[3]. 하지만 플러딩 공격의 경우 공격 특성 상 인터넷의 DDoS (Distributed Denial of Service) 공격과 유사하여 공격자의 위치가 노출되지 않고 정상 메시지와 비정상 메시지의 구별이 어렵다. 이를 위해 SIP 프로토콜의 특성을 이용한 플러딩 공격에 대한 탐지 및 대응 기법들이 제안되고 있다. 참고문헌 [4], [5], [6]에서는 플러딩 공격에 대한 탐지 기법을 제안하고 있으나 유동적인 네트워크 상황을 반영하기 힘든 점과 탐지 이후의 대응에는 미흡한 면이 있다. 참고문헌 [7]과 [8]에서는 필터링 기반의 대응 기법이 제안되어 있으나, 구조의 복잡성과 기존의 정상적인 사용자의 세션을 보호하기 힘들다는 단점이 있다. 이를 극복하기 위해 화이트리스트를 이용하여 정상적인 사용자를 보호하는 기법[6]이 제안 되었으나 다양한 종류의 플러딩 공격에 대응하지 못하는 한계를 갖는다.

본 논문에서는 블룸필터[13]를 사용하여 화이트리스트를 구성하고 이를 사용하여 정상적인 사용자를 보호하기 위한 방법을 제안한다. 제안 방법은 세션 설정 과정을 이용하여 정상적인 세션구성이 완료된 사용자들을 기준으로 하여 화이트리스트를 구성함으로써 다양한 종류의 플러딩 공격 시에도 효과적으로 정상 사용자를 보호할 수 있다. 또한, 블룸필터를 이용함으로써 많은 양의 사용자 데이터를 줄여서 공간 효율적으로 빠르게 검색 할 수 있다는 장점이 있다.

본 논문의 구성은 다음과 같다. 제2장에서는 본 논문의 배경이 되는 관련 연구에 대해 간략히 소개하고, 제3장에서는 제안방법에 대하여 기술한다. 그리고, 제4장 에서는 제안된 방법의 성능을 평가하고, 제5장에서는 결론을 맺는다.

Ⅱ. 관련 연구

2.1 SIP (Session Initiation Protocol)

SIP는 IETF RFC 3261에 규정된 VoIP와 같은 인터넷상에서의 멀티미디어 응용 서비스의 세션을 구성하고 관리하기 위하여 사용되는 시그널링 프로토콜이다[9]. SIP는 세션을 설정하고, 이를 제어하기 위한 다양한 명령어들을 정의한다. SIP의 메시지 구조는 HTTP와 유사한 텍스트 기반의 구조를 가지고 있으며, 이것은 요청 및 응답 메시지로 쌍을 이뤄 동작한다. SIP 메시지는 헤더와 바디로 구성되어 있으며, 헤더는 SIP 시그널링 정보를 포함하고 바디는 호 설정 시 오디오 및 비디오 코덱과 같은 부가정보를 제공한다.

그림 1은 SIP 세션 설정 과정을 보여준다. 송신자(caller) 는 수신자 (callee) 에게 세션을 생성하기 위한 INVITE 메시지를 보내게 된다. INVITE 메시지를 전달 받은 프록시 서버는 메시지를 통해 수신자를 인식하고 받은 메시지를 적절한 수신자로 전달하게 된다. INVITE 메시지를 받은 수신자는 이에 대한 응답으로서 200 OK 메시지를 보내게 된다. 응답을 받은 발신자는 이를 제대로 받았음을 알리기 위해 ACK 메시지를 송신함으로써 하나의 세

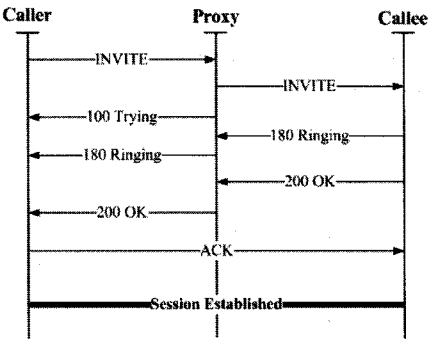


그림 1. SIP Session Setup 과정

션이 생성된다. 본 논문에서는 이와 같이 INVITE/200 OK/ACK의 3-way handshake가 정상적으로 이루어진 세션을 기준으로 화이트리스트를 구성하게 되며 이는 3장에서 기술하기로 한다.

2.2 SIP에서의 서비스 거부 공격

SIP는 인터넷 환경에서 운용되므로, 일반적인 인터넷상에서의 위협과 유사한 서비스 거부 공격에 노출되어 있다. SIP에서의 서비스 거부 공격의 목적은 시스템이 정상적인 동작을 하지 못하게 하는 측면에서 인터넷에서의 그것과 유사하지만 가장 큰 차이점은 공격의 방법이 SIP 메시지를 기반으로 한다는 점에 있다. SIP 서비스 거부 공격은 다음과 같이 3가지로 구분할 수 있다[10].

- Malformed 메시지 공격: 정상적인 SIP 메시지를 전송하는 것이 아니라, 공격자에 의해 의도적으로 조작된 메시지를 프록시 서버에 전송함으로써 소프트웨어 취약점을 노려 프록시가 제 기능을 하지 못하도록 하는 공격이다.
- 기본 SIP Flood 공격: 공격자는 SIP 패킷 헤더에 임의의 정보를 넣은 다수의 패킷을 생성하여 프록시 서버에 전송함으로써 대역폭, CPU 사용량, 메모리 등의 시스템 자원을 고갈시킴으로써 서비스 거부에 빠지게 하는 공격이다. 주로 INVITE, REGISTER 메시지를 이용한다.
- 향상된 SIP Spoof Flood 공격: 다수의 패킷을 생성하여 프록시 서버에 전송하여 시스템 자원을 고갈시키는 것은 기본 SIP Flood 공격과 유사하나, 공격 SIP 패킷 헤더의 내용을 임의의 정보가 아닌 적합한 사용자의 정보를 이용하여 작성한다는 차이점이 있다. 적합한 사용자의 정보를 사용하기에 공격을 탐지 및 대응하기 어렵고, 기본 SIP Flood 공격에 비해 더 많은 시스템 자원을 소모한다.

2.3 기존의 서비스 거부 대응 기법

플러딩 공격으로 인한 서비스 거부 대응 기법은 공격 탐지와 대응으로 나뉜다. SIP 플러딩 공격을 탐지하기 위해 CUSUM[4]을 이용한 방안과, 헬링거 거리 (Hellinger distance)[5]를 이용한 방안, 가변 임계치(adaptive threshold)[6]를 이용한 방안이 제안되어 있으나 정상상태의 트래픽을 기반으로 탐지하고 있어 지속적으로 변화하는 네트워크 상황을 반영하지 못하고 있다. 이를 극복하기 위하여, 정상적인 상태에서 발생 가능한 메시지 상한값을 예측하여 SIP 플러딩 공격을 탐지하는 기법[11]이 제안되어 있다.

공격 대응 기법은 일반적으로 필터링 기법이 이용된다. 필터링 기법은 블랙리스트를 이용한 공격 메시지를 선별하는 방법과 화이트리스트를 이용한 정상 메시지를 허용하는 방법이 연구되었다. IDS (Intrusion Detection System)을 이용하여 공격 탐지 시 공격 사용자에 대한 블랙리스트를 생성하여 공격자로부터 가장 가까운 라우터에게 이 목록을 전달하여 필터링 하는 기법이 제안되었다[7]. 이는 공격자가 발생시키는 다수의 플러딩 메시지를 메시지 발생 지점에서 봉쇄하여 네트워크 자원을 낭비하지 않는 다는 장점이 있지만, IDS를 사용해야만 함으로써 발생하는 오버헤드와 네트워크의 모든 라우터에서 제안 기법이 동작해야만 필터링을 할 수 있다는 한계점을 갖는다. 이러한 부가적인 오버헤드를 줄이기 위해 SIP 프록시 서버 앞에서 히스토리 기반의 IP 필터링 기법을 제안되었다[8]. 이는 SIP 세션을 자주 맺는 사용자들을 화이트리스트로 정의하여 공격 시 새로운 요청에 대해 화이트리스트에 있으면 요청을 허용하는 방법이다. 하지만 SIP 세션을 자주 맺는 사용자들의 리스트를 사전에 구축해야만 하고, 세션을 자주 맺는 사용자들에 대한 정의의 모호성을 갖는다. 이에 대응하여 SIP의 REGISTER 메시지를 이용하여 정상 사용자들에 대한 화이트리스트를 작성하는 기법이 제안되었다[12]. SIP 등록 서버에 정상적인 등록 과정을 거친 사용자를 화이트리스트로 구성하여 서비스 거부 공격 시 화이트리스트에 있는 사용자들에 대해서만 요청을 허용하는 기법이다. 하지만 정상적으로 REGISTER 과정을 거친 공격자에 대해서는 공격을 막을 수 없다는 한계가 있다.

2.4 블룸필터

블룸필터는 통계적 특성을 가진 자료구조로서 많은 양의 데이터를 줄여서 공간 효율적으로 빠르게 검색을 할 수 있는 장점을 갖는다[13]. 블룸필터는 그림 2와 같이 해시 함수(hash function)들을 사용하여 어떤 집합의 원소에 대한 멤버쉽 테스트, 즉 그 원소가 집합의 멤버에 속하느냐 속하지 않느냐를 빠르게 계산해 줄 수 있다. 블룸필터의 기본적인 동작은 다음과 같다.

블룸필터는 m개의 bit로 구성되고, k개의 독립적인 해시 함수로부터 블룸필터가 구성된다. 초기에

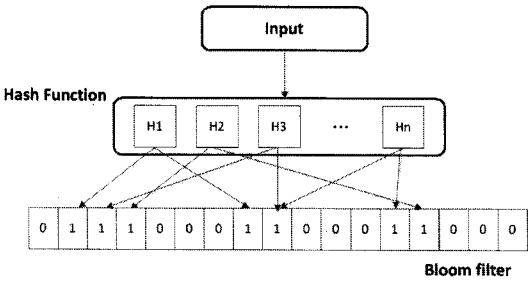


그림 2. 기본 블룸필터 구조

블룸필터의 모든 bit은 0으로 설정된다. 새로운 메시지가 주어질 때마다, 이 메시지를 k개의 해시 함수에 적용되고 이로부터 k개의 결과값, 즉 블룸필터 인덱스가 산출된다. 산출된 k개의 결과값에 해당하는 블룸필터의 위치를 1로 설정한다.

이러한 과정을 통하여 블룸필터가 구성되고, 이를 사용하여 이후 진입되는 메시지의 소속여부를 다음과 같이 판단하게 된다. 메시지가 주어지면, 이를 k개의 해시 함수에 적용하여 결과값들을 구하고, 이 결과값들에 해당하는 블룸필터 인덱스의 bit값이 모두 1로 설정되어 있는지를 확인하다. 모든 인덱스들의 비트값이 1로 설정되어 있는 경우, 이 메시지는 멤버에 속하여 있다고 판단되며, 이와 반대로 어느 하나라도 0이 있게 되면 이 메시지는 기존 멤버가 아닌 신규로 진입한 메시지로 구분되게 된다.

Ⅲ. 제안 방법

본 논문에서는 SIP 기반의 VoIP 서비스에서 대부분의 사용자가 이미 자신이 알고 있거나 이전에 세션을 형성하였던 사용자들과의 다시 세션을 구성할 가능성이 크다는 가정[14]에 기반하여 정상적인 세션 설정 과정을 맺은 사용자들을 화이트리스트로 구성하여 서비스 거부 공격에 대응하는 기법을 제안한다.

3.1 전체 시스템 구조

본 논문에서 제안하는 시스템 구조를 그림 3에 나타내었다. 프록시 서버 앞에 화이트리스트를 관리하는 Verifier 모듈과 정상 메시지들을 분류하기 위한 Filter 모듈로 구성되어 있고, 이들의 동작은 다음과 같다.

- Verifier 모듈은 블룸필터를 이용한 화이트리스트를 생성 및 관리하기 위한 모듈이다. 화이트리스트 생성을 위해 현재 세션을 맺기 위해 대기하고 있는 사용자들의 정보를 유지하고 정상적으로 세션을 설정한다면 해당 사용자의 정보를 화이트리스트에 추가한다.
- Filter 모듈은 프록시 서버로 들어오는 SIP 메시지를 관찰하고 서비스 거부 공격 시 Verifier 모듈의 화이트리스트를 이용하여 화이트리스트에 있는 사용자들의 SIP 패킷은 통과 시키고 화이트리스트에 없는 사용자의 패킷은 공격자로 분류, 패킷을 폐기함으로써 정상적인 사용자들을 보호하는 기능을 수행한다. 또한 현재 진행 중인 세션 정보를 Verifier로 전달해 줌으로써 화이트리스트 구성을 돕는다.
- SIP 프록시 서버는 송신자의 SIP 요청 메시지를 처리하여 수신자에게 전달하고 수신자로부터 요청에 대한 수락 메시지를 받으면 이를 송신자로 전달하는 등의 SIP 세션의 생성 및 관리 기능을 수행한다.

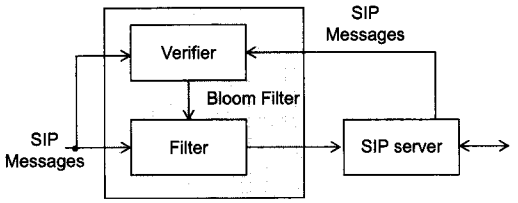


그림 3. 전체 시스템 구조

3.2 Verifier : 화이트리스트 구성

일반적으로 화이트리스트 또는 블랙리스트는 네트워크 관리자 혹은 시스템 관리자로부터 미리 정해진 사용자 리스트를 받게 되고 이를 기반으로 필터링을 수행하게 된다. 이 경우 새로운 사용자의 정보를 적용하기 힘들다는 점과 네트워크 상의 유동적인 변화를 반영하기 힘들다는 점이 있다.

이를 극복하기 위하여 제안 방법은 성공적으로 세션이 구성된 사용자 정보를 모니터링 하여 화이트리스트를 구성한다. 화이트리스트 구성 시 시스템의 부하를 줄이고, 검색 시간 등의 장점[13]을 취하기 위해 블룸필터를 이용한다. 제안하는 화이트리스트 구성 방법은 다음과 같다.

3.2.1 정상 세션의 추출

그림 1에서와 같이 정상적인 세션은 INVITE, 200 OK, ACK가 순차적으로 교환되어 이루어진다.

① Verifier 모듈에서는 INVITE 메시지가 수신되

면, 이로부터 <송신자 IP 주소, 수신자 IP 주소, 송신자 ID (from), 수신자 ID (to)>로 이루어진 세션정보를 추출하여 저장한다.

② 수신자가 INVITE에 대한 200OK 응답을 보내면, 서버가 이를 받게 되고, 서버는 이 200 OK 메시지를 송신자뿐만이 아니라 Verifier에게도 전달한다. Verifier는 세션 정보를 추출하여, 이전에 저장된 세션정보들중에서 이의 존재 여부를 확인하고, 존재할 경우 이를 마킹하여 둔다.

③ 송신자는 200 OK에 대한 응답으로 ACK를 보내게 되고, 이 ACK를 Verifier도 수신하게 된다. Verifier는 세션정보를 추출하고 이전에 존재하는 세션정보들과 비교하여, ①과 ②의 단계를 거친 세션정보가 존재하면, 이 세션은 정상적으로 구성된 것으로 최종 판단을 하게 된다.

3.2.2 화이트리스트 구성

그림 4는 정상세션에 대하여 화이트리스트를 구성하는 과정을 보여준다. 정상적으로 구성된 세션정보는 <송신자 IP 주소, 수신자 IP 주소, 송신자 ID (from), 수신자 ID (to)>가 하나의 스트링으로서 표현된다. 이 정상세션에 대한 세션 스트링을 k개의 해시함수에 적용하고 이로부터 나온 k개의 결과값에 해당하는 블룸필터의 위치를 1로 기록한다. 블룸필터가 갱신될 때마다 Verifier는 이를 Filter에 제공한다.

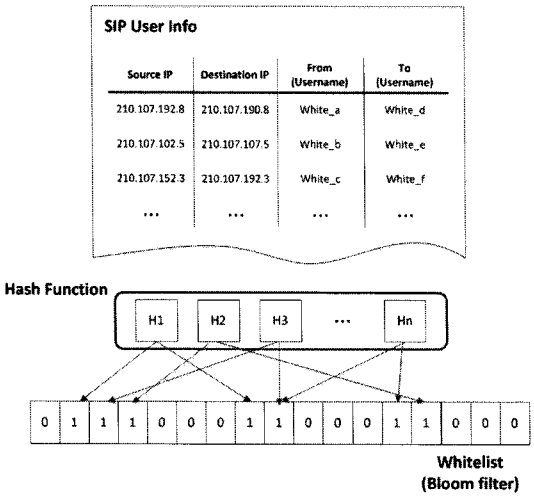


그림 4. 블룸필터를 이용한 화이트리스트 구조

3.3 SIP 서비스 거부 공격 대응 알고리즘

SIP 플러딩 공격과 같은 서비스거부 공격의 탐지는 기존의 방법들[4]-[6],[11]들 중에서 사용하는 것을 가정한다.

세션에 관련된 메시지는 Filter 모듈을 거쳐 프록시 서버로 유입된다. 서비스 거부 공격이 탐지 되지 않은 경우, 모든 메시지는 서버에게 전달된다. 그러나 서비스 공격이 탐지된 경우는 그림 5와 같은 과정을 통하여 대응하게 된다.

서비스공격이 탐지된 경우, Filter는 Verifier에게 화이트리스트를 요청한다. Verifier는 가장 최신에 구성된 화이트리스트를 Filter 모듈로 전달한다. Filter는 이를 이용하여 들어온 요청 메시지에서 <송신자 IP 주소, 수신자 IP 주소, 송신자 ID (from), 수신자 ID (to)>를 추출하고 이를 화이트리스트 입력값으로 만들게 된다. 만들어진 입력값은 그림 6의 서비스 거부 알고리즘을 따라 해시함수를 통해 각각의 화이트리스트 블룸필터의 인덱스 값으로 대응되게 된다. 인덱스 값을 이용해 화이트리스트 내의 해당 위치의 값을 확인하고 이것이 모두 1일 경우 해당 요청 메시지는 이전에 정상적인 세션을 맺은 사용자, 즉 정상 사용자임을 확인할 수 있다. 정상 사용자의 메시지로 확인된다면 해당 메시지를 서버 모듈로 전달하여 새로운 세션을 맺도록 한다. 만약 하나라도 1이 아닌 경우 이것은 화이트리스트 내의 사용자가 아닌 공격자로 판단하고, Filter는 해당 메시지를 폐기함으로써, 서비스 거부 공격 상황에서도 정상 사용자는 안정적으로 SIP 서비스를 제공받을 수 있게 된다.

```
an SIP message arrives at Filter;
if ( an attack symptom is detected ) then
  extract session information of the message;
  for each hash function (j=1,2,···,k)
    if (the bit position in the whitelist of j-th
      hash result != 1) then
        DROP the message and RETURN;
    endif
  endfor
endif
FORWARD the message to the SIP server;
```

그림 5. 서비스 거부 대응 알고리즘

Ⅳ. 성능 평가

제안방법의 정확도는 블룸필터의 크기와 해시 함수의 수에 좌우된다[13]. 시스템의 복잡성을 고려하여 해시함수의 개수를 5개로 가정하였다. 해시함수의 개수가 5개일 때, 20,000개의 엔트리를 적용하였을 때의 블룸필터 크기에 대한 오탐율 (false-positive ratio)를 그림 6에 나타내었다. 약 0.1%의 오탐율을 목표치로 가정하였을 때, 블룸필터 크기가 약 240 Kbit 이상에서 부터 목표치를 달성할 수 있음을 관찰하여, 블룸필터의 크기를 240 Kbit로 설정하였다. 블룸필터의 크기를 240 Kbit로 하여, 해시함수 개수에 따른 오탐율을 그림 7과 같이 구하였다. 본 논문에서 정한 해시함수 5개 이상에서부터 오탐율이 0.1% 이하가 됨을 확인 할 수 있다. 이로부터, 제안방법에 적용할 블룸필터의 크기는 240 Kbit, 해시함수의 개수는 5개로 정하였다.

앞에서 정의한 블룸필터를 사용한 제안 방법에 대한 성능 평가를 위하여, 네트워크 시뮬레이터인 OPNET[17]을 사용하여 가상의 SIP 네트워크 환경을 구성하였다.

SIP 정상 사용자와 공격자의 트래픽 발생을 다음과 같이 하였다. 정상 사용자 트래픽은 SIPp[15]를 참조하여 OPNET 시뮬레이터 상에서 구현하였다. 정상 사용자로 부터의 메시지 발생은 평균적으로 초당 60개 메시지가 지수함수분포에 따라 이루어지는 것으로 정하였다.

공격 메시지는 INVITE Flooder[16]를 참조하여 구현하였다. SIP 플러딩 공격을 위하여 공격자는 송신자 인터넷 주소, 수신자 인터넷 주소, 송신자 아이디, 수신자 아이디, 세션 아이디를 무작위로 바꾸어 가며 SIP 메시지를 생성하도록 하였다. 공격 메시지들은 평균 초당 600 메시지가 지수함수분포에 따라 발생하는 것으로 가정하였다.

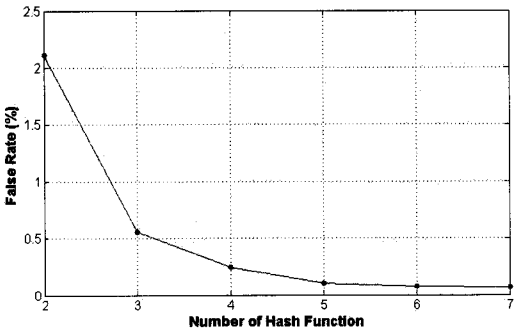


그림 7. 해시함수 수에 따른 오탐율 (m=240000)

그림 8은 실험을 위하여 정상트래픽과 공격트래픽을 혼합하여 발생시킨 패턴을 보여준다. 정상트래픽은 평균 초당 60개의 메시지가 전시간대에 걸쳐 발생되고 있고, 공격트래픽은 평균 초당 600개의 메시지 발생율을 갖고 1800~2400초 구간에서 활성화 되도록 하였다.

제안방법이 적용되지 않은 경우, 이들 그림 8의 메시지들은 모두 서버에 도달하게 되고, 공격이 활성화된 구간에서 서버가 수용 가능한 범위이상의 메시지가 유입되면, 서버는 서비스가 불가한 상태가 될 수 있다.

반면에, 제안방법이 적용된 상황에서의 서버에 도달하는 메시지의 수를 그림 9에 나타내었다. 공격이 시작된 초기에 공격을 탐지하는데 소요된 시간에서의 일부 메시지수 증가가 관찰되고, 이후에는 모든 공격 메시지들이 Filter에서 제거되므로, 서버에는 정상 메시지들만 유입되어 서버가 정상적으로 서비스가 이루어지게 된다.

그림 10은 화이트리스트를 기존의 리스트에 기반하여 구성하여 검색하는 방식[8]과 제안된 블룸필터를 이용하여 화이트리스트를 사용하여 검색하는 경

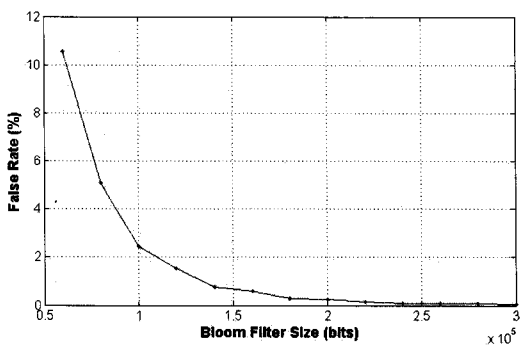


그림 6. 블룸필터 크기에 따른 오탐율 (k=5)

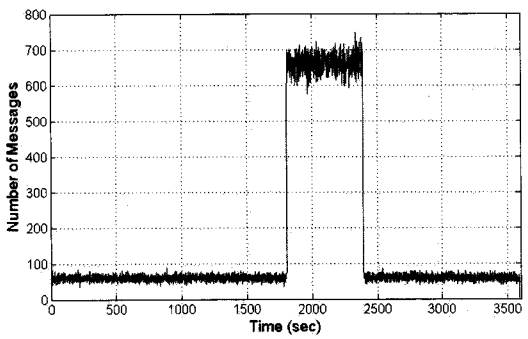


그림 8. 서버에 유입되는 메시지 량(필터 미동작시)

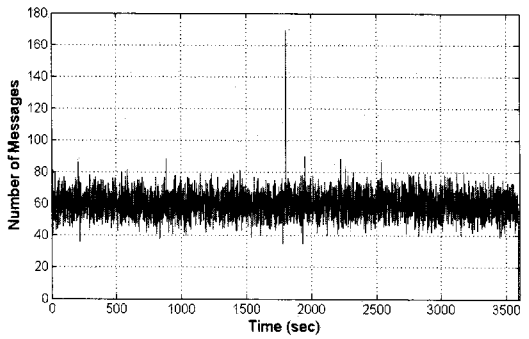


그림 9. 서버에 유입되는 메시지 량 (제안방법을 적용한 필터 동작시)

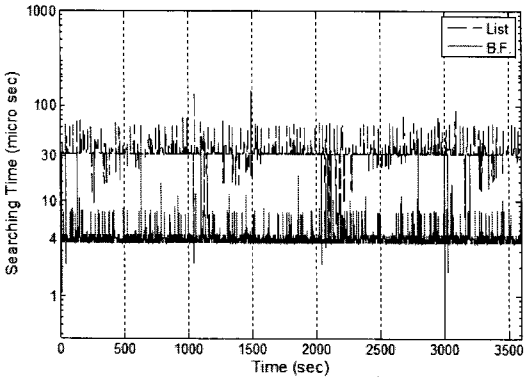


그림 10. 리스트 방식과 블룸필터의 검색 시간

우에 대한 메시지 검색 시간을 나타내었다. 실선은 기존의 리스트 방식을 이용하여 구성했을 때의 검색 시간으로서, 점선으로 나타낸 제안한 블룸필터를 적용했을 때의 검색 시간에 비하여 약 8배 이상의 차이가 나타나는 것을 볼 수 있다. 일반적으로 리스트기반의 방식의 검색시간의 복잡성은 리스트의 크기에 비례하는 O(log m)의 특징을 보여주는데 비하여, 블룸필터에 의한 검색시간은 해시함수 계산의 시간만 요구되므로 리스트의 크기에 무관한 O(1)의 성능을 보여주게 된다.

V. 결 론

본 논문에서는 블룸필터를 이용하여 화이트리스트를 사용함으로써 SIP 서비스 거부 공격에 효과적으로 대응할 수 있는 방법을 제안하였다. 본 논문에서 제안하는 방법은 기존에 정상 세션을 설정한 이력을 기반으로 화이트리스트를 구성하므로, 기존의 방법들에서는 대응하기 힘들었던 다양한 SIP 플러딩에 의한 서비스 공격 방법에 대응 가능하다. 제안 방법을 적용함으로써, 공격 상황에서도 정상적인 메시지들은 보호를 받고 서비스가 가능함으로, 안정적인 SIP 서비스 제공에 기여 가능하다. 앞으로, 보다 실질적인 상황을 고려하여 다중 공격 형식의 고려와 여러 공격의 중첩 시 대응할 수 있는 방안에 대해 지속적인 연구를 진행하고자 한다.

참 고 문 헌

[1] P. Lawecki, "VoIP Security in Public Networks," Alcatel Lucent, Feb., 2007.

[2] A. Bremler-Barr, R. Halachmi-Bekel, "Unregister attacks in SIP," NPSEC 2006, Nov., 2006.

[3] D. Geneiatakis, et al., "A lightweight protection mechanism against signaling attacks in a SIP based VoIP environment", Telecommunication System, Vol.36, No.4, pp.153-159, Dec., 2007.

[4] Y. Rebahi et al., "Detecting Flooding Attack against IP Multimedia Subsystem(IMS) Network," AICCSA Apr., 2008.

[5] H. Sengar et al., "Detecting VoIP Floods Using the Hellinger Distance", IEEE Tr.Parallel and Distributed Systems, Vol.19, No.6, June, 2008.

[6] V. Siris and F. Papagalou, "Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks," Computer Communications, Vol.29, No.9, pp.1433-1442, 2006.

[7] F. Huici, S. Niccolini, N. d'Heureuse, "Protecting SIP against Very Large Flooding DoS Attacks," IEEE GLOBECOM 2009. Dec., 2009

[8] C. Zhou, C. Leckie, K. Ramamohanarao, "Protecting SIP server from CPU-based DoS attacks using history-based IP filtering," IEEE Communications Letters, Vol.13, No.10, pp.800-802, Oct., 2009

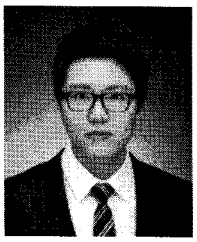
[9] J.Rosenberg et al "SIP : Session Initiation Protocol", IETF RFC 3261, June, 2002

[10] M. Luo, T. Peng, C. Leckie, "CPU-based DoS attacks against SIP servers," IEEE NOMS 2008

[11] J. Ryu, K. Ryu, B. Roh, "Detection of SIP Flooding Attacks based on the Upper Bound of the Possible Number of SIP Messages" KSII Transactions on Internet and Information

Systems Vol.3 No.5, pp.507-526 Oct., 2009
[12] E.Y. Chen, M. Itoh, "A whitelist approach to protect SIP servers from flooding attacks," IEEE CQR 2010, June, 2010.
[13] D. Guo, J. Wu, H. Chen, Y. Yuan, X. Luo, "The Dynamic Bloom Filters," IEEE Tr. Knowledge and Data Engineering, Vol.22, No.1, pp.120-133, Jan., 2010.
[14] X. Deng, M. Shore, "Advanced Flooding Attack on a SIP Server," IEEE ARES 2009, Mar., 2009.
[15] R. Gayraud, O. Jacques, "SIPp", available at http://sipp.sourceforge.net
[16] VOIPSA, Packet Creation and Flooding Tools, http://voipsa.org/Resources/tools.php#VoIPOPNET, http://www.opnet.com

김 주 완 (Ju-Wan Kim) 준회원



2009년 아주대학교 정보컴퓨터공학부 (공학사)
2011년 아주대학교 일반대학원 컴퓨터공학과 (공학석사)
<관심분야> 이동 멀티미디어 통신 네트워크 프로토콜, OPNET 모델링&시뮬레이션, 국방전술 네트워크 등

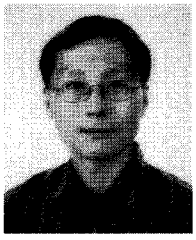
류 제 택 (Jea-Tek Ryu) 정회원

2005년 아주대학교 정보컴퓨터공학부 (공학사)
2007년 아주대학교 정보통신전문대학원 (공학석사)
2011년 아주대학교 정보통신전문대학원 (공학박사)
2011년~현재 한국특허정보원
<관심분야> 유/무선 인터넷 멀티미디어 통신 및 응용, 유비쿼터스 네트워킹, 네트워크 보안, 센서 네트워크 등

류 기 열 (Ki-Yeol Ryu) 정회원

1985년 서울대학교 컴퓨터공학과 (공학사)
1987년 한국과학기술원 전산학과 (공학석사)
1992년 한국과학기술원 전산학과 (공학박사)
1993년~1994년 동경대 전산학과 연구원
1994년~현재 아주대학교 정보컴퓨터공학부 부교수
<관심분야> 유비쿼터스 컴퓨팅, 서비스 지향 컴퓨팅, 컴포넌트 모델 및 프레임 워크, 객체지향 프로그래밍 언어, 분산 오브젝트 시스템, RFID 시스템 등

노 병 희 (Byeong-hee Roh) 종신회원



1987년 한양대학교 전자공학과 (공학사)
1989년 한국과학기술원 전기및 전자공학과(공학석사)
1998년 한국과학기술원 전기및 전자공학과(공학박사)
1989년~1994년 한국통신 통신망 연구소
1998년~2000년 삼성전자
2000년~현재 아주대학교 정보통신전문대학원 교수
2005년 Stony Brook University 방문교수
<관심분야> 멀티미디어 네트워크 및 응용, 유무선 네트워크 QoS 및 트래픽 엔지니어링, 유비쿼터스 센서 네트워크(RFID/USN), 인터넷 보안, 국방전술통신네트워크 등