



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0095155
(43) 공개일자 2018년08월27일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) H04L 12/26 (2006.01)
H04L 29/08 (2006.01)

(52) CPC특허분류
H04L 63/1458 (2013.01)
H04L 43/16 (2013.01)

(21) 출원번호 10-2017-0021018
(22) 출원일자 2017년02월16일
심사청구일자 2017년02월16일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자
김희강
서울특별시 서초구 태봉로2길 65 404동 302호 (우면동, 네이처힐4단지)

이현승
경기도 고양시 덕양구 화신로 291, 1011동 1502호 (화정동, 별빛마을10단지아파트)

송현민
서울특별시 성북구 안암로9가길 87-6 (안암동5가)

(74) 대리인
김동용, 김홍석

전체 청구항 수 : 총 11 항

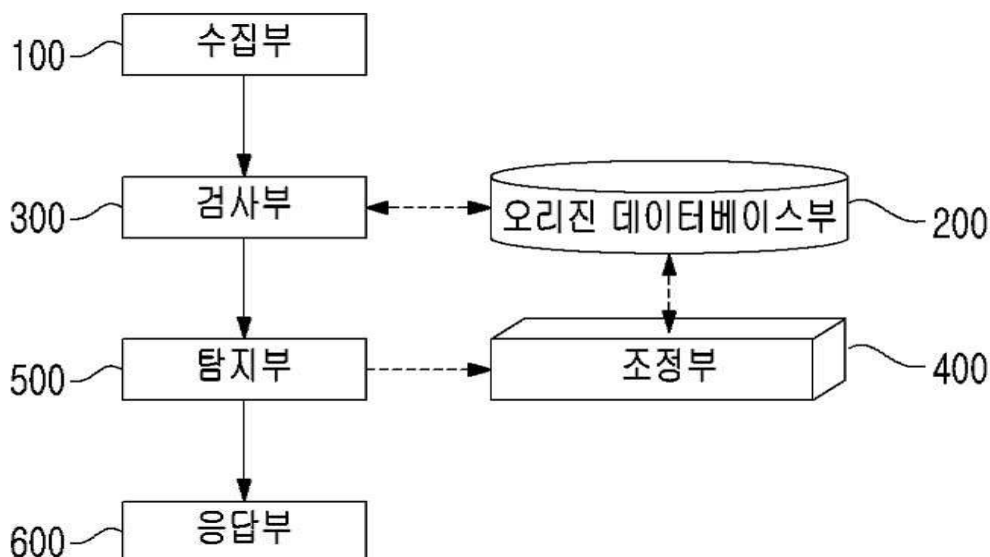
(54) 발명의 명칭 웹소켓 서버의 오리진 관리 시스템 및 방법

(57) 요약

본 발명은 공격자가 봇넷을 이용하여 동시에 대상 서버로 웹소켓 연결을 대량으로 발생시켜 대상 서버의 과부하를 유발하는 DDoS 공격을 효과적으로 탐지하고 방어할 수 있는 웹소켓 서버의 오리진 관리 시스템 및 방법을 제공한다.

(뒷면에 계속)

대표도 - 도4



이를 위해, 본 발명의 실시예에 따른 웹소켓 서버의 오리진 관리 시스템은, 웹소켓 구조를 갖는 하나 이상의 클라이언트와 상기 웹소켓 구조를 가지며 클라이언트가 접속하는 서버를 포함하고, 서버는, 클라이언트로부터 웹소켓 연결 요청이 있을 때 클라이언트의 오리진(origin) 정보를 수집하는 수집부, 오리진 정보를 블랙리스트, 화이트리스트 및 그레이리스트로 구분하여 저장하는 오리진 데이터베이스부, 수집부를 통해 수집한 클라이언트 오리진 정보가 오리진 데이터베이스부의 블랙리스트에 포함되면 해당 클라이언트의 웹소켓 연결을 차단하고 TCP 연결을 거부하고, 화이트리스트에 포함되면 해당 클라이언트의 웹소켓 연결을 허용하는 검사부, 수집한 클라이언트 오리진 정보가 그레이리스트에 포함되면, 소정 단위 시간 마다 상기 오리진으로부터의 웹소켓 연결수 및 전송 받는 데이터양을 각각 측정하고, 측정한 연결수에 기초한 제1 임계값 및 상기 측정한 데이터양에 기초로 제2 임계값을 결정하는 조정부, 오리진으로부터의 웹소켓 연결수가 제1 임계값을 초과하거나 전송 받는 데이터양이 상기 제2 임계값을 초과하면 해당 오리진에 대한 추가적인 연결을 차단하고, 초과하지 않으면 해당 클라이언트의 웹소켓 연결을 허용하는 탐지부, 탐지부의 탐지 결과를 클라이언트 및 서버에 전송하는 응답부를 포함하는 것을 특징으로 한다.

이를 통해, 오리진에 대한 블랙리스트와 화이트리스트를 정의하여 사용자의 연결 허용 여부를 결정하고 새로운 오리진의 연결 요청을 지속적으로 검사하여, 해당 연결 요청을 시스템에서 허용 또는 거부할지 판단하는 과정을 통해 웹소켓 서버를 겨냥한 DDoS 공격을 효과적으로 방어할 수 있다.

(52) CPC특허분류

H04L 63/101 (2013.01)

H04L 63/1416 (2013.01)

H04L 67/02 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 B01011602300004003

부처명 미래창조과학부

연구관리전문기관 정보통신기술진흥센터

연구사업명 정보통신방송연구개발사업

연구과제명 스크립트 기반 사이버 공격 사전 예방 및 대응 기술 개발

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2016.03.01 ~ 2017.02.28

명세서

청구범위

청구항 1

웹소켓이 적용되는 하나 이상의 클라이언트와

상기 웹소켓이 적용되며 상기 클라이언트가 접속하는 서버를 포함하고,

상기 서버는,

상기 클라이언트로부터 웹소켓 연결 요청이 있을 때 상기 클라이언트의 오리진(origin) 정보를 수집하는 수집부,

상기 오리진 정보를 블랙리스트, 화이트리스트 및 그레이리스트로 구분하여 저장하는 오리진 데이터베이스부,

상기 수집부를 통해 수집한 클라이언트 오리진 정보가 상기 오리진 데이터베이스부의 블랙리스트에 포함되면 해당 클라이언트의 웹소켓 연결을 차단하고 TCP 연결을 거부하고, 화이트리스트에 포함되면 해당 클라이언트의 웹소켓 연결을 허용하는 검사부,

상기 수집한 클라이언트 오리진 정보가 상기 그레이리스트에 포함되면, 소정 단위 시간 마다 상기 오리진으로부터의 웹소켓 연결수 및 전송 받는 데이터양을 각각 측정하고, 상기 측정한 연결수에 기초한 제1 임계값 및 상기 측정한 데이터양에 기초한 제2 임계값을 결정하는 조정부,

상기 오리진으로부터의 웹소켓 연결수가 상기 제1 임계값을 초과하거나 상기 전송 받는 데이터양이 상기 제2 임계값을 초과하면 해당 오리진에 대한 추가적인 연결을 차단하고, 초과하지 않으면 해당 클라이언트의 웹소켓 연결을 허용하는 탐지부,

상기 탐지부의 탐지 결과를 상기 클라이언트 및 서버에 전송하는 응답부를 포함하는 것을 특징으로 하는 웹소켓 서버의 오리진 관리 시스템.

청구항 2

제1 항에 있어서,

상기 조정부는,

상기 수집한 클라이언트 오리진 정보가 상기 그레이리스트에 포함되면 상기 수집한 클라이언트 오리진 정보로 상기 오리진 데이터베이스부를 업데이트하고, 포함되지 않으면 상기 수집한 클라이언트 오리진 정보를 상기 오리진 데이터베이스부의 그레이리스트에 추가하는 것을 특징으로 하는 웹소켓 서버의 오리진 관리 시스템.

청구항 3

제1 항에 있어서,

상기 조정부는,

상기 소정 단위 시간 마다 측정한 복수 개의 웹소켓 연결수의 평균값(μ_1) 및 표준편차값(σ_1)에 기초하여 상기 제1 임계값을 결정하고, 상기 소정 단위 시간 마다 측정한 복수 개의 데이터양의 평균값(μ_2) 및 표준편차값(σ_2)에 기초하여 상기 제2 임계값을 결정하는 것을 특징으로 하는 웹소켓 서버의 오리진 관리 시스템.

청구항 4

제1 항에 있어서,

상기 조정부는,

상기 소정 단위 시간 마다 웹소켓 연결수 및 데이터양이 측정되지 않는 클라이언트 오리진의 경우, 상기 그레이리스트에 포함된 모든 오리진의 연결수 및 데이터양에 기초하여 제1 임계값 및 제2 임계값을 결정하는 것을 특

징으로 하는 웹소켓 서버의 오리진 관리 시스템.

청구항 5

제4 항에 있어서,

상기 조정부는,

상기 제1 임계값 및 제2 임계값을 시간의 경과에 따라 갱신하는 것을 특징으로 하는 웹소켓 서버의 오리진 관리 시스템.

청구항 6

제3 항에 있어서,

상기 조정부는,

상기 제1 임계값(Threshold₁)을 아래의 수식을 통해 결정하는 것을 특징으로 하는 웹소켓 서버의 오리진 관리 시스템.

$$\text{Threshold}_1 = \mu_1 + 3\sigma_1$$

청구항 7

제3 항에 있어서,

상기 조정부는,

상기 제2임계값(Threshold₂)을 아래의 수식을 통해 결정하는 것을 특징으로 하는 웹소켓 서버의 오리진 관리 시스템.

$$\text{Threshold}_2 = \mu_2 + 3\sigma_2$$

청구항 8

서버가 클라이언트로부터 웹소켓 연결 요청이 있을 때 상기 클라이언트의 오리진(origin) 정보를 수집하는 제1 단계;

상기 수집한 오리진 정보를 블랙리스트, 화이트리스트 및 그레이리스트로 구분하여 오리진 데이터베이스부에 저장하는 제2 단계;

상기 수집한 클라이언트 오리진 정보가 상기 오리진 데이터베이스부의 블랙리스트에 포함되면 해당 클라이언트의 웹소켓 연결을 차단하고 TCP 연결을 거부하고, 화이트리스트에 포함되면 해당 클라이언트의 웹소켓 연결을 허용하는 제3 단계;

상기 수집한 클라이언트 오리진 정보가 상기 그레이리스트에 포함되면, 소정 단위 시간 마다 상기 오리진으로부터의 웹소켓 연결수 및 전송 받는 데이터양을 각각 측정하고, 상기 측정한 연결수에 기초한 제1 임계값 및 상기 측정한 데이터양에 기초로 제2 임계값을 결정하는 제4 단계;

상기 오리진으로부터의 웹소켓 연결수가 상기 제1 임계값을 초과하거나 상기 전송 받는 데이터양이 상기 제2 임계값을 초과하면 해당 오리진에 대한 추가적인 연결을 차단하고, 초과하지 않으면 해당 클라이언트의 웹소켓 연결을 허용하는 제5 단계;

상기 제5 단계의 결과를 상기 클라이언트 및 서버에 전송하는 제6 단계를 포함하는 것을 특징으로 하는 웹소켓 서버의 오리진 관리 방법.

청구항 9

제8 항에 있어서,

상기 제4 단계는,

상기 수집한 클라이언트 오리진 정보가 상기 그레이리스트에 포함되면 상기 수집한 클라이언트 오리진 정보로

상기 오리진 데이터베이스부를 업데이트하고, 포함되지 않으면 상기 수집한 클라이언트 오리진 정보를 상기 오리진 데이터베이스부의 그레이리스트에 추가하는 것을 특징으로 하는 웹소켓 서버의 오리진 관리 방법.

청구항 10

제8 항에 있어서,

상기 제4 단계는,

소정 단위 시간 마다 측정한 복수 개의 웹소켓 연결수의 평균값(μ_1) 및 표준편차값(σ_1)에 기초하여 상기 제1 임계값을 결정하고, 상기 소정 단위 시간 마다 측정한 복수 개의 데이터양의 평균값(μ_2) 및 표준편차값(σ_2)에 기초하여 상기 제2 임계값을 결정하는 것을 특징으로 하는 웹소켓 서버의 오리진 관리 방법.

청구항 11

제8 항에 있어서,

상기 제4 단계는,

상기 소정 단위 시간 마다 웹소켓 연결수 및 데이터양이 측정되지 않는 클라이언트 오리진의 경우, 상기 그레이리스트에 포함된 모든 오리진의 연결수 및 데이터양에 기초하여 제1 임계값 및 제2 임계값을 결정하고, 상기 제1 임계값 및 제2 임계값을 시간의 경과에 따라 갱신하는 것을 특징으로 하는 웹소켓 서버의 오리진 관리 방법.

발명의 설명

기술 분야

[0001] 본 발명은 웹소켓 서버의 오리진 관리 시스템 및 방법에 관한 것으로, 자세하게는 웹소켓 프로토콜이 동일 오리진 정책(same-origin policy)을 차용하지 않음에 따라 발생할 가능성이 있는 보안적 문제점을 효과적으로 해결할 수 있는 웹소켓 서버의 오리진 관리 시스템 및 방법에 관한 것이다.

배경 기술

[0002] HTML5가 발표되기 전의 서버와 클라이언트 간 통신 방법은 폴링과 포스트백 방식이었다. 폴링은 전송할 데이터의 유무에 관계없이 주기적으로 요청을 수행하는 방식이고, 포스트백은 클라이언트가 서버에 정보를 요청하면 서버가 응답을 하는 GET, POST 방식이었다. 또한 Ajax를 사용하여 웹 페이지의 특정 부분에 대해서만 요청하여 다시 로딩하는 방식이 있었다.

[0003] 이러한 통신 방법은 비교적 높은 오버헤드를 요구하거나 요청이 없으면 응답할 수 없다는 단점이 존재하였다.

[0004] HTML5 도입 후 지속적인 양방향 통신을 지원하는 웹소켓 프로토콜이 발표되었다. 서버와 사용자 사이에서 웹소켓을 통한 연결이 이루어지는 경우, 요청과 응답 과정 없이 원하는 쪽에서 데이터 전송이 가능한 진정한 동시성이 제공될 수 있다.

[0005] 또한 웹소켓 프로토콜은 기존의 기술과 다르게 낮은 오버헤드를 요구하며, 간단한 인터페이스를 통해 연결이 가능하다는 장점이 존재한다.

[0006] 또한, 웹소켓 서버는 연결 요청을 받을 때 클라이언트의 오리진 헤더(origin header)를 확인할 수 있다. 여기서 오리진이란 도 1에 도시된 바와 같이, 스킴(scheme), 호스트(host), 포트(port)로 구성되며 스킴은 HTTP 혹은 웹소켓과 같은 프로토콜을 말하고, 호스트는 도메인 주소를 말한다. 두 개의 오리진이 있을 때 스킴, 호스트 그리고 포트 번호 중 하나라도 다를 경우 다른 오리진으로 취급된다. 그리고 웹소켓은 동일 오리진 정책(same-origin policy)을 차용하지 않았기 때문에 다른 오리진에서 온 요청도 허용이 가능하다. 여기서 동일 오리진 정책이란, 한 출처(Origin)에서 로드된 문서나 스크립트가 다른 출처 자원과 상호작용하지 못하도록 제한하며 동일 오리진의 경우에만 접근을 허가하는 정책 또는 어떤 오리진 A가 B라는 문서 객체 모델(document object model)에 접근할 때 같은 오리진이 아니라면 접근할 수 없는 정책을 말한다. 구체적으로 도 2에 도시된 예와 같이 두 개의 오리진이 서로 다른 오리진일 경우에 상호간의 접근이 허용되지 않는다. 도 2의 경우에는 호스트가 상이하여 다른 오리진으로 취급되는 것을 도시하고 있다.

[0007] 또한, 동일 오리진 여부를 판단하는 예는 아래 표 1과 같다.

[0008] [표 1]

비교 URL	결과	이유
http://shop.example.com/dir2/other.html	O	동일 출처 (Same origin)
https://shop.example.com/another.html	X	프로토콜 상이
http://shop.example.com:81/dir/etc.html	X	포트번호 상이
http://news.example.com/dir/other.html	X	호스트 상이

[0009]

[0010]

여기서 기준이 되는 오리진은 http://shop.example.com/dir/page.html 이다.

[0011]

표 1에 도시된 바와 같이, 첫 번째, 완전히 동일한 출처인 경우(스킵, 호스트, 포트번호가 모두 동일)에는 동일 오리진으로 판단하고, 두 번째, 프로토콜이 상이한 경우에는 다른 오리진으로 판단하고, 세 번째, 포트번호가 상이한 경우에는 다른 오리진으로 판단하고, 네 번째, 호스트가 상이한 경우에 다른 오리진으로 판단한다.

[0012]

또한, 웹소켓 프로토콜은 연결 과정(handshake) 동안 동일 오리진 정책을 차용하지 않기 때문에 서버와 다른 도메인에서 연결 요청을 보낼 수 있고, 이에 따라 서버 관리자 측에서는 웹소켓 어플리케이션을 구축할 때 연결을 요청하는 클라이언트가 악의적인 사용자인지 검증하는 과정이 꼭 필요하다.

[0013]

즉, 오리진을 이용하면 서버 측이 허용하고 싶지 않은 연결을 거절할 수 있다. 다시 말해서 서버는 수신되는 요청의 오리진 헤더를 조사하여, 악의적으로 판단되는 연결 요청은 처리하지 않기로 할 수 있다. 하지만 악의적인 연결을 요청하는 오리진을 판별하기 힘든 경우에는 전체적으로 연결되는 웹소켓의 수를 제한하는 방식의 통제가 필요하게 된다. 따라서 정당한 클라이언트에 대해서도 연결이 거부되거나 단절될 수 있기 때문에 상기에서 언급한 종래 방식들로는 유연하게 대처할 수 없는 문제점이 존재한다.

[0014]

또한, 외부의 공격자는 목표로 정한 웹소켓 서버를 무력화시키기 위해 본인의 페이지에 접속한 클라이언트들을 봇넷(botnet)으로 감염시켜, 타겟 서버의 웹소켓 프로토콜에 연결되도록 조작할 수 있다.

[0015]

이러한 경우, 만약 웹소켓의 오리진을 통제하지 않는 서버는, 어떠한 도메인에서 접속을 요청해도 연결을 허용한다. 따라서 공격자가 감염된 봇넷을 이용해 DDoS 공격을 수행하면 일시에 많은 양의 웹소켓 연결이 발생하게 되어 목표 서버가 결국 공격을 당하는 상태가 될 수 있다.

[0016]

기존 웹소켓 DDoS 공격에 대한 방어 기술은, 전체 웹소켓 연결 양을 시스템의 환경에 따라 제한하거나 오리진에 대한 블랙리스트 목록을 정의하여 특정 오리진에서 온 요청을 거절하는 방법 등이 사용되고 있다. 하지만 블랙리스트에 포함되지 않은 오리진에서 공격이 이루어지면 서버는 손쉽게 무력화될 가능성이 있기 때문에 알려지지 않은 오리진에 대한 방어 기법에 대한 기술 개발이 절실히 요구되고 있는 실정이다.

선행기술문헌

특허문헌

[0017]

(특허문헌 0001) 대한민국 공개특허 제2016-0067449호(2016.06.14 공개)

발명의 내용

해결하려는 과제

[0018]

본 발명의 실시예는 공격자가 봇넷을 이용하여 동시에 대상 서버로 웹소켓 연결을 대량으로 발생시켜 대상 서버의 과부하를 유발하는 DDoS 공격을 효과적으로 탐지하고 방어할 수 있는 웹소켓 서버의 오리진 관리 시스템 및 방법을 제공하는 것에 목적이 있다.

[0019]

본 발명이 해결하고자 하는 과제는 이상에서 언급된 과제로 제한되지 않는다. 언급되지 않은 다른 기술적 과제들은 이하의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

- [0020] 본 발명의 실시예에 따른 웹소켓 서버의 오리진 관리 시스템은, 웹소켓이 적용되는 하나 이상의 클라이언트와 상기 웹소켓이 적용되며 상기 클라이언트가 접속하는 서버를 포함하고, 상기 서버는, 상기 클라이언트로부터 웹소켓 연결 요청이 있을 때 상기 클라이언트의 오리진(origin) 정보를 수집하는 수집부, 상기 오리진 정보를 블랙리스트, 화이트리스트 및 그레이리스트로 구분하여 저장하는 오리진 데이터베이스부, 상기 수집부를 통해 수집한 클라이언트 오리진 정보가 상기 오리진 데이터베이스부의 블랙리스트에 포함되면 해당 클라이언트의 웹소켓 연결을 차단하고 TCP 연결을 거부하고, 화이트리스트에 포함되면 해당 클라이언트의 웹소켓 연결을 허용하는 검사부, 상기 수집한 클라이언트 오리진 정보가 상기 그레이리스트에 포함되면, 소정 단위 시간 마다 상기 오리진으로부터의 웹소켓 연결수 및 전송 받는 데이터양을 각각 측정하고, 상기 측정한 연결수에 기초한 제1 임계값 및 상기 측정한 데이터양에 기초로 제2 임계값을 결정하는 조정부, 상기 오리진으로부터의 웹소켓 연결수가 상기 제1 임계값을 초과하거나 상기 전송 받는 데이터양이 상기 제2 임계값을 초과하면 해당 오리진에 대한 추가적인 연결을 차단하고, 초과하지 않으면 해당 클라이언트의 웹소켓 연결을 허용하는 탐지부, 상기 탐지부의 탐지 결과를 상기 클라이언트 및 서버에 전송하는 응답부를 포함하는 것을 특징으로 한다.
- [0021] 또한, 상기 조정부는, 상기 수집한 클라이언트 오리진 정보가 상기 그레이리스트에 포함되면 상기 수집한 클라이언트 오리진 정보로 상기 오리진 데이터베이스부를 업데이트하고, 포함되지 않으면 상기 수집한 클라이언트 오리진 정보를 상기 오리진 데이터베이스부의 그레이리스트에 추가하는 것을 특징으로 한다.
- [0022] 또한, 상기 조정부는, 상기 소정 단위 시간 마다 측정한 복수 개의 웹소켓 연결수의 평균값(μ_1) 및 표준편차값(σ_1)에 기초하여 상기 제1 임계값을 결정하고, 상기 소정 단위 시간 마다 측정한 복수 개의 데이터양의 평균값(μ_2) 및 표준편차값(σ_2)에 기초하여 상기 제2 임계값을 결정하는 것을 특징으로 한다.
- [0023] 또한, 상기 조정부는, 상기 소정 단위 시간 마다 웹소켓 연결수 및 데이터양이 측정되지 않는 클라이언트 오리진의 경우, 상기 그레이리스트에 포함된 모든 오리진의 연결수 및 데이터양에 기초하여 제1 임계값 및 제2 임계값을 결정하는 것을 특징으로 한다.
- [0024] 또한, 상기 조정부는, 상기 제1 임계값 및 제2 임계값을 시간의 경과에 따라 갱신하는 것을 특징으로 한다.
- [0025] 또한, 상기 조정부는, 상기 제1 임계값(Threshold₁)을 아래의 수식을 통해 결정하는 것을 특징으로 한다.
- [0026]
$$\text{Threshold}_1 = \mu_1 + 3\sigma_1$$
- [0027] 또한, 상기 조정부는, 상기 제2임계값(Threshold₂)을 아래의 수식을 통해 결정하는 것을 특징으로 한다.
- [0028]
$$\text{Threshold}_2 = \mu_2 + 3\sigma_2$$
- [0029] 본 발명의 실시예에 따른 웹소켓 서버의 오리진 관리 방법은, 서버가 클라이언트로부터 웹소켓 연결 요청이 있을 때 상기 클라이언트의 오리진(origin) 정보를 수집하는 제1 단계; 상기 수집한 오리진 정보를 블랙리스트, 화이트리스트 및 그레이리스트로 구분하여 오리진 데이터베이스부에 저장하는 제2 단계; 상기 수집한 클라이언트 오리진 정보가 상기 오리진 데이터베이스부의 블랙리스트에 포함되면 해당 클라이언트의 웹소켓 연결을 차단하고 TCP 연결을 거부하고, 화이트리스트에 포함되면 해당 클라이언트의 웹소켓 연결을 허용하는 제3 단계; 상기 수집한 클라이언트 오리진 정보가 상기 그레이리스트에 포함되면, 소정 단위 시간 마다 상기 오리진으로부터의 웹소켓 연결수 및 전송 받는 데이터양을 각각 측정하고, 상기 측정한 연결수에 기초한 제1 임계값 및 상기 측정한 데이터양에 기초로 제2 임계값을 결정하는 제4 단계; 상기 오리진으로부터의 웹소켓 연결수가 상기 제1 임계값을 초과하거나 상기 전송 받는 데이터양이 상기 제2 임계값을 초과하면 해당 오리진에 대한 추가적인 연결을 차단하고, 초과하지 않으면 해당 클라이언트의 웹소켓 연결을 허용하는 제5 단계; 상기 제5 단계의 결과를 상기 클라이언트 및 서버에 전송하는 제6 단계를 포함하는 것을 특징으로 한다.
- [0030] 또한, 상기 제4 단계는, 상기 수집한 클라이언트 오리진 정보가 상기 그레이리스트에 포함되면 상기 수집한 클라이언트 오리진 정보로 상기 오리진 데이터베이스부를 업데이트하고, 포함되지 않으면 상기 수집한 클라이언트 오리진 정보를 상기 오리진 데이터베이스부의 그레이리스트에 추가하는 것을 특징으로 한다.
- [0031] 또한, 상기 제4 단계는, 소정 단위 시간 마다 측정한 복수 개의 웹소켓 연결수의 평균값(μ_1) 및 표준편차값(σ_1)에 기초하여 상기 제1 임계값을 결정하고, 상기 소정 단위 시간 마다 측정한 복수 개의 데이터양의 평균값(μ_2)

2) 및 표준편차값(σ_2)에 기초하여 상기 제2 임계값을 결정하는 것을 특징으로 한다.

[0032] 또한, 상기 제4 단계는, 상기 소정 단위 시간 마다 웹소켓 연결수 및 데이터양이 측정되지 않는 클라이언트 오리진의 경우, 상기 그레이리스트에 포함된 모든 오리진의 연결수 및 데이터양에 기초하여 제1 임계값 및 제2 임계값을 결정하고, 상기 제1 임계값 및 제2 임계값을 시간의 경과에 따라 갱신하는 것을 특징으로 한다.

발명의 효과

[0033] 본 발명의 일 측면에 따르면, 오리진에 대한 블랙리스트와 화이트리스트를 정의하여 사용자의 연결 허용 여부를 결정하고 새로운 오리진의 연결 요청을 지속적으로 검사하여, 해당 연결 요청을 시스템에서 허용 또는 거부할지 판단하는 과정을 통해 웹소켓 서버를 겨냥한 DDoS 공격을 효과적으로 방어할 수 있다.

[0034] 또한, 기존 서버에서는 알지 못하는 새로운 오리진에 대해서 유연한 대처가 이루어질 수 있도록 한다.

[0035] 또한, 클라이언트의 브라우저 환경에 의존할 필요가 없기 때문에 범용적으로 서버의 안전성 유지가 가능하도록 할 수 있다.

[0036] 본 발명의 효과는 상술한 효과들로 제한되지 않는다. 언급되지 않은 효과들은 본 명세서 및 첨부된 도면으로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확히 이해될 수 있을 것이다.

도면의 간단한 설명

[0037] 도 1은 오리진의 구성을 도시한 도면이다.

도 2는 다른 오리진으로 웹소켓 서버에 연결한 예를 도시한 도면이다.

도 3은 웹소켓 구조를 갖는 클라이언트와 서버 사이에서 발생하는 웹소켓 연결 요청 및 대응 과정을 도시한 도면이다.

도 4는 본 발명의 실시예에 따른 웹소켓 서버의 오리진 관리 시스템의 서버 구성을 도시한 블록도이다.

도 5는 본 발명의 실시예에 따른 웹소켓 서버의 오리진 관리 방법의 과정을 도시한 순서도이다.

도 6은 본 발명의 실시예에 따른 웹소켓 서버의 오리진 관리 시스템에서 소정 단위 시간 마다 측정된 복수 개의 웹소켓 연결수 및 데이터양에 대한 정규분포를 도시한 그래프이다.

발명을 실시하기 위한 구체적인 내용

[0038] 본 발명의 다른 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술하는 실시 예를 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시 예에 한정되지 않으며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 만일 정의되지 않더라도, 여기서 사용되는 모든 용어들(기술 혹은 과학 용어들을 포함)은 이 발명이 속한 종래 기술에서 보편적 기술에 의해 일반적으로 수용되는 것과 동일한 의미를 갖는다. 공지된 구성에 대한 일반적인 설명은 본 발명의 요지를 흐리지 않기 위해 생략될 수 있다. 본 발명의 도면에서 동일하거나 상응하는 구성에 대하여는 가급적 동일한 도면부호가 사용된다. 본 발명의 이해를 돕기 위하여, 도면에서 일부 구성은 다소 과장되거나 축소되어 도시될 수 있다.

[0039] 본 발명에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다", "가지다" 또는 "구비하다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0040] 본 명세서 전체에서 사용되는 '~부'는 적어도 하나의 기능이나 동작을 처리하는 단위로서, 예를 들어 소프트웨어, FPGA 또는 ASIC과 같은 하드웨어 구성요소를 의미할 수 있다. 그렇지만 '~부'가 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. '~부'는 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다.

[0041] 일 예로서 '~부'는 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트

트들, 드라이버들, 펌웨어, 마이크로 코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함할 수 있다. 구성요소와 '~부'에서 제공하는 기능은 복수의 구성요소 및 '~부'들에 의해 분리되어 수행될 수도 있고, 다른 추가적인 구성요소와 통합될 수도 있다.

- [0042] 본 발명의 실시예에 따라 제공되는 웹소켓 서버의 오리진 관리 시스템 및 방법은, 도 3에 도시된 상황에서 서버 측에서 클라이언트의 웹소켓 연결 요청을 수락할지 거절할지, 해당 오리진을 분석하여 효율적으로 수락 또는 거절 여부를 결정하도록 하기 위한 보다 개선된 프로토콜을 제안한다.
- [0043] 도 3은 웹소켓 구조를 갖는 클라이언트와 서버 사이에서 발생하는 웹소켓 연결 요청 및 대응 과정을 도시한 도면이다.
- [0044] 이하에서는, 첨부되는 도면을 참조하여 본 발명의 실시예들에 대해 구체적으로 설명한다.
- [0045] 먼저 본 발명의 실시예에 따른 웹소켓 서버의 오리진 관리 시스템의 구성에 대해 도 4를 기초로 이하에서 살펴본다. 도 4는 본 발명의 실시예에 따른 웹소켓 서버의 오리진 관리 시스템의 서버 구성을 도시한 블록도이다.
- [0046] 본 발명의 실시예에 따른 웹소켓 서버의 오리진 관리 시스템은, 웹소켓 구조를 갖는 하나 이상의 클라이언트와 웹소켓 구조를 가지며 클라이언트가 접속하는 서버로 이루어진다.
- [0047] 또한, 도 4에 도시된 바와 같이 서버는, 수집부(100), 오리진 데이터베이스부(200), 검사부(300), 조정부(400), 탐지부(500) 및 응답부를 포함한다.
- [0048] 수집부(100)는 클라이언트로부터 웹소켓 연결 요청이 있을 때 클라이언트의 오리진(origin) 정보를 수집한다.
- [0049] 또한, 오리진 데이터베이스부(200)는 오리진 정보를 블랙리스트, 화이트리스트 및 그레이리스트로 구분하여 저장한다. 여기서 블랙리스트에 포함되는 오리진은 웹소켓 연결을 허용하지 말아야 하는 오리진에 해당한다. 그리고 화이트리스트에 포함되는 오리진은 웹소켓 연결을 허용해도 무방한 오리진에 해당한다. 그레이리스트에 포함되는 오리진은 웹소켓 연결 여부를 판단할 수 없는 오리진에 해당한다.
- [0050] 또한, 오리진 데이터베이스부(200)가 상기와 같은 세 가지 리스트를 구분하는 기준은 미리 설정된 데이터 정보 또는 갱신되어 저장되는 오리진의 정보를 기초로 설정될 수 있다.
- [0051] 또한, 검사부(300)는 수집부(100)를 통해 수집한 클라이언트 오리진 정보가 오리진 데이터베이스부(200)의 블랙리스트에 포함되면 해당 클라이언트의 웹소켓 연결을 차단하고 TCP 연결을 거부하고, 화이트리스트에 포함되면 해당 클라이언트의 웹소켓 연결을 허용한다.
- [0052] 또한, 조정부(400)는 수집한 클라이언트 오리진 정보가 그레이리스트에 포함되면, 소정 단위 시간 마다 오리진으로부터의 웹소켓 연결수 및 전송 받는 데이터양을 각각 측정하고, 측정된 연결수에 기초한 제1 임계값 및 측정된 데이터양에 기초로 제2 임계값을 결정한다.
- [0053] 또한, 조정부(400)는 수집한 클라이언트 오리진 정보가 그레이리스트에 포함되면 수집한 클라이언트 오리진 정보로 오리진 데이터베이스부(200)를 업데이트하고, 포함되지 않으면 수집한 클라이언트 오리진 정보를 오리진 데이터베이스부(200)의 그레이리스트에 추가한다.
- [0054] 또한, 조정부(400)는 소정 단위 시간 마다 측정한 복수 개의 웹소켓 연결수의 평균값(μ_1) 및 표준편차값(σ_1)에 기초하여 제1 임계값을 결정하고, 소정 단위 시간 마다 측정한 복수 개의 데이터양의 평균값(μ_2) 및 표준편차값(σ_2)에 기초하여 제2 임계값을 결정한다.
- [0055] 또한, 조정부(400)는 소정 단위 시간 마다 웹소켓 연결수 및 데이터양이 측정되지 않는 클라이언트 오리진의 경우, 그레이리스트에 포함된 모든 오리진의 연결수 및 데이터양에 기초하여 제1 임계값 및 제2 임계값을 결정한다.
- [0056] 또한, 조정부(400)는 상기에서 결정한 제1 임계값 및 제2 임계값을 시간의 경과에 따라 갱신할 수 있다.
- [0057] 또한, 조정부(400)는 제1 임계값(Threshold₁)을 아래의 수식 1을 통해 결정할 수 있다.
- [0058] Threshold₁ = $\mu_1 + 3\sigma_1$
- [0059] 또한, 조정부(400)는 제2임계값(Threshold₂)을 아래의 수식 2를 통해 결정할 수 있다.

- [0060] $\text{Threshold}_2 = \mu_2 + 3\sigma_2$
- [0061] 또한, 탐지부(500)는 오리진으로부터의 웹소켓 연결수가 제1 임계값을 초과하거나 전송 받는 데이터양이 제2 임계값을 초과하면 해당 오리진에 대한 추가적인 연결을 차단하고, 초과하지 않으면 해당 클라이언트의 웹소켓 연결을 허용한다.
- [0062] 또한, 응답부(600)는 탐지부(500)의 탐지 결과(해당 오리진에 대한 연결 차단 결과 또는 연결 허용 결과)를 클라이언트 및 서버에 전송한다.
- [0063] 이상에서는 본 발명의 실시예에 따른 웹소켓 서버의 오리진 관리 시스템의 서버 구성에 대해 살펴보았고, 각 서버 구성 간의 동작 과정에 대해서는 아래의 웹소켓 서버의 오리진 관리 방법 과정을 기초로 상세히 설명한다.
- [0064] 본 발명의 실시예에 따른 웹소켓 서버의 오리진 관리 방법은, 서버가 클라이언트로부터 웹소켓 연결 요청이 있을 때 클라이언트의 오리진(origin) 정보를 수집하는 제1 단계, 수집한 오리진 정보를 블랙리스트, 화이트리스트 및 그레이리스트로 구분하여 오리진 데이터베이스부에 저장하는 제2 단계, 수집한 클라이언트 오리진 정보가 오리진 데이터베이스부의 블랙리스트에 포함되면 해당 클라이언트의 웹소켓 연결을 차단하고 TCP 연결을 거부하고, 화이트리스트에 포함되면 해당 클라이언트의 웹소켓 연결을 허용하는 제3 단계, 수집한 클라이언트 오리진 정보가 그레이리스트에 포함되면, 소정 단위 시간 마다 오리진으로부터의 웹소켓 연결수 및 전송 받는 데이터양을 각각 측정하고, 측정한 연결수에 기초한 제1 임계값 및 측정한 데이터양에 기초로 제2 임계값을 결정하는 제4 단계, 오리진으로부터의 웹소켓 연결수가 제1 임계값을 초과하거나 전송 받는 데이터양이 제2 임계값을 초과하면 해당 오리진에 대한 추가적인 연결을 차단하고, 초과하지 않으면 해당 클라이언트의 웹소켓 연결을 허용하는 제5 단계 및 제5 단계의 결과를 클라이언트 및 서버에 전송하는 제6 단계로 이루어질 수 있다.
- [0065] 여기서 제4 단계는, 수집한 클라이언트 오리진 정보가 그레이리스트에 포함되면 수집한 클라이언트 오리진 정보로 오리진 데이터베이스부를 업데이트하고, 포함되지 않으면 수집한 클라이언트 오리진 정보를 오리진 데이터베이스부의 그레이리스트에 추가한다.
- [0066] 또한, 제4 단계는, 소정 단위 시간 마다 측정한 복수 개의 웹소켓 연결수의 평균값(μ_1) 및 표준편차값(σ_1)에 기초하여 제1 임계값을 결정하고, 소정 단위 시간 마다 측정한 복수 개의 데이터양의 평균값(μ_2) 및 표준편차값(σ_2)에 기초하여 제2 임계값을 결정한다.
- [0067] 또한, 제4 단계는, 소정 단위 시간 마다 웹소켓 연결수 및 데이터양이 측정되지 않는 클라이언트 오리진의 경우, 그레이리스트에 포함된 모든 오리진의 연결수 및 데이터양에 기초하여 제1 임계값 및 제2 임계값을 결정하고, 제1 임계값 및 제2 임계값을 시간의 경과에 따라 갱신한다.
- [0068] 마지막으로, 본 발명의 실시예에 따른 웹소켓 서버의 오리진 관리 방법의 구체적인 과정에 대해 도 5 내지 도 6을 기초로 살펴보면 다음과 같다.
- [0069] 도 5는 본 발명의 실시예에 따른 웹소켓 서버의 오리진 관리 방법의 과정을 도시한 순서도이고, 도 6은 본 발명의 실시예에 따른 웹소켓 서버의 오리진 관리 시스템에서 소정 단위 시간 마다 측정한 복수 개의 웹소켓 연결수 및 데이터양에 대한 정규분포를 도시한 그래프이다.
- [0070] 도 5에 도시된 바와 같이, 본 발명의 실시예에 따른 웹소켓 서버의 오리진 관리 방법 과정에서 먼저 웹소켓 연결 요청에 대한 클라이언트 오리진 정보를 수집한다(S10). 그런 후 수집한 오리진 정보를 블랙리스트, 화이트리스트 및 그레이리스트로 구분하여 저장한다(S11).
- [0071] 그리고, 해당 오리진이 블랙리스트나 화이트리스트에 포함되는지 여부를 판단한다(S12). 만약 블랙리스트나 화이트리스트에 포함되는 경우에는 다시 해당 오리진이 블랙리스트에 포함되는지 판단한다(S13). 해당 오리진이 블랙리스트에 포함된 경우에는 해당 클라이언트 웹소켓 연결을 차단하고 TCP 연결을 거부하고(S14), 웹소켓 연결 실패 응답 메시지를 클라이언트와 서버로 전송한다(S30). 만약 화이트리스트에 포함된 경우에는 웹소켓 연결을 허용하고(S15), 웹소켓 연결 성공 응답 메시지를 클라이언트와 서버로 전송한다(S31).
- [0072] 만약 해당 오리진이 블랙리스트나 화이트리스트에 포함되지 않는 경우에는 해당 오리진이 그레이리스트에 포함되는지 여부를 판단한다(S20). 포함되지 않는 경우에는 수집된 오리진 정보를 오리진 데이터베이스에 추가하고(S22), 웹소켓 연결을 유지하면서 성공 응답 메시지를 클라이언트 및 서버에 전송한다(S31).
- [0073] 만약 그레이리스트에 포함되는 경우에는 수집된 오리진 정보를 오리진 데이터베이스 상에서 업데이트하고(S21),

다시 해당 오리진의 연결수 및 데이터양을 제1 임계값 및 제2 임계값과 비교한다. 즉, 해당 오리진의 연결수가 제1 임계값을 초과하거나 해당 오리진의 데이터양이 제2 임계값을 초과하는지 여부를 판단한다(S23). 연결수 또는 데이터양 중 어느 하나가 제1 임계값 또는 제2 임계값을 초과하는 경우라면 해당 오리진에 대한 추가적인 연결을 차단하고(S24), 웹소켓 연결 실패 응답 메시지를 클라이언트와 서버에 전송한다(S30). 여기서 제1 임계값 및 제2 임계값 설정에 대해서는 아래에서 상술한다.

[0074] 그리고, 연결수 또는 데이터양 중 어느 하나가 제1 임계값 또는 제2 임계값을 초과하는 경우가 아니라면, 웹소켓 연결을 허용하고(S25), 웹소켓 연결 성공 응답 메시지를 클라이언트와 서버에 전송한다.

[0075] 상기 제1 임계값 및 제2 임계값에 대해 상세히 설명하면, 본 발명의 실시예에 따른 웹소켓 서버의 오리진 관리 시스템의 서버 구성 중 조정부(400)가, 적절한 단위 시간(분 또는 시간)마다 각 오리진의 연결 수와 전송받은 데이터의 양을 측정한다.

[0076] 그리고 조정부(400)는 단위 시간 블록($t_{i-9} \sim t_i$)까지 각 오리진의 연결 수와 데이터양 각각에 대한 평균값(μ)과 표준편차값(σ)을 계산한다. 이렇게 구해진 단위 시간 블록의 평균값과 표준편차값을 이용하여 다음 단위 시간(t_{i+1})동안 각 오리진에 대한 허용 가능한 연결 수와 데이터의 양을 결정하여 각 오리진에 대한 큐(queue)의 크기를 결정한다.

[0077] 구체적으로, 시간 블록($t_{i-9} \sim t_i$)에 대한 정규분포를 그려보면 도 6과 같다. 즉, 본 발명의 실시예에 따른 시스템에서 t_{i+1} 의 시간동안 가능한 웹소켓 연결 수의 임계값인 제1 임계값은 $Threshold_1 = \mu_1 + 3\sigma_1$ 로 결정할 수 있고, 허용 가능한 데이터 양의 임계값인 제2 임계값은 $Threshold_2 = \mu_2 + 3\sigma_2$ 로 결정할 수 있다.

[0078] 그 결과 t_{i+1} 시간에 대한 변화 허용 범위는 이전 단위 블록 값들의 평균값과 비교하여 약 99%의 변화까지 수용할 수 있게 된다.

[0079] 만약 $t_{i-9} \sim t_i$ 의 단위 시간 동안 발견되지 않았던 오리진이 t_{i+1} 시간에 발생한다면 해당 오리진의 임계값을 그레이리스트에 포함된 모든 오리진의 연결 수와 데이터양의 평균값과 표준편차값을 상기와 같은 기준(평균값과 표준편차값의 3배의 합)에 기초하여 초기 임계값을 설정할 수 있다.

[0080] 결론적으로, 특정 오리진에 대하여 t_{i+1} 단위 시간동안 연결 수 또는 데이터 전송량이 제1 임계값 또는 제2 임계값을 초과한다면 추가적인 연결 및 데이터의 수신을 거부한다. 그리고 각각의 오리진에 대한 유동적인 임계값(제1 임계값 및 제2 임계값)을 조정하여 해당 오리진의 연결 및 데이터 전송량이 임계값보다 낮아졌을 때 다시 추가적인 연결을 허용할 수 있다.

[0081] 구체적으로 임계값을 결정하는 과정은 아래와 같다.

[0082] n 개의 시간 블록에 대한 평균값(μ)과 표준편차값(σ)을 계산할 수 있는데 평균값, 표준편차값 및 임계값(Threshold)의 계산 과정은 아래 수식을 통해 이루어진다.

[0083]

$$\mu = \frac{\sum_{j=1}^n t_{i+j-1}}{n}$$

[0084]

$$\sigma = \sqrt{\frac{\sum_{j=1}^n (t_{i+j-1} - \mu)^2}{n}}$$

[0085]

$$Threshold = \mu + 3\sigma = \frac{\sum_{j=1}^n t_{i+j-1}}{n} + 3\sqrt{\frac{\sum_{j=1}^n (t_{i+j-1} - \mu)^2}{n}}$$

[0086] 마지막으로, 본 발명의 실시예가 적용된 예를 아래에서 설명한다.

[0087] 아래 표 2에서 나타난 바와 같이, 소정 단위 시간(t) 마다 해당 클라이언트 오리진(www.normal.com)의 웹소켓 연결수와 수신 데이터 총량을 측정한다. 그리고, 총 10개의 시간 구간($t_1 \sim t_{10}$)에 대해 연결수 및 데이터 양을 측정한다. 물론 해당 클라이언트 오리진은 블랙리스트나 화이트리스트에 포함되지 않는 오리진에 해당한다.

[0088] [표 2]

오리진		t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9	t_{10}
www.normal.com	웹소켓 연결 수	26	44	50	20	48	79	68	50	33	40
	수신 데이터 총량	40	77	102	55	141	210	183	110	59	66

[0089]

[0090] 측정한 연결수와 데이터 양에 대해, 이 10이므로 $t_1 \sim t_{10}$ 의 평균값(μ)과 표준편차값(σ)을 구하면,

[0091] 웹소켓 연결 수에 대한 평균값과 표준편차값은 각각 45.8과 17.01이고, 수신 데이터 총량에 대한 평균값과 표준편차값은 각각 54.39와 104.3로 계산됩니다.

[0092] 여기서 t_{11} 의 임계값을 아래 식을 통해 결정하면,

[0093] $\text{Threshold} = \mu + 3\sigma$

[0094] 제1 임계값은 97이고, 제2 임계값은 366으로 결정될 수 있다.

[0095] 결국, 해당 단위 시간(t_{11}) 동안 해당 오리진의 연결수가 제1 임계값을 넘거나, 해당 오리진의 데이터 총량이 제2 임계값을 넘는 연결이 발생하면, 본 시스템은 이상이 있는 것으로 탐지하고 해당 오리진의 웹소켓 연결을 제한할 수 있다.

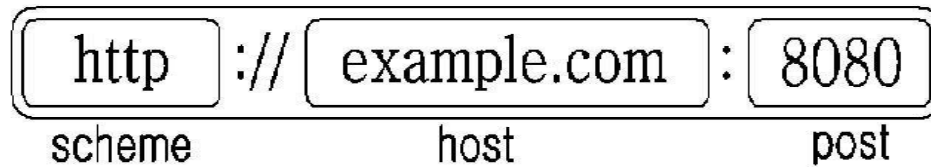
[0096] 이상의 실시 예들은 본 발명의 이해를 돕기 위하여 제시된 것으로, 본 발명의 범위를 제한하지 않으며, 이로부터 다양한 변형 가능한 실시 예들도 본 발명의 범위에 속하는 것임을 이해하여야 한다. 본 발명의 기술적 보호범위는 특허청구범위의 기술적 사상에 의해 정해져야 할 것이며, 본 발명의 기술적 보호범위는 특허청구범위의 문언적 기재 그 자체로 한정되는 것이 아니라 실질적으로는 기술적 가치가 균등한 범주의 발명에 대하여까지 미치는 것임을 이해하여야 한다.

부호의 설명

[0097] 100 : 수집부
200 : 오리진 데이터베이스부
300 : 검사부
400 : 조정부
500 : 탐지부
600 : 응답부

도면

도면1

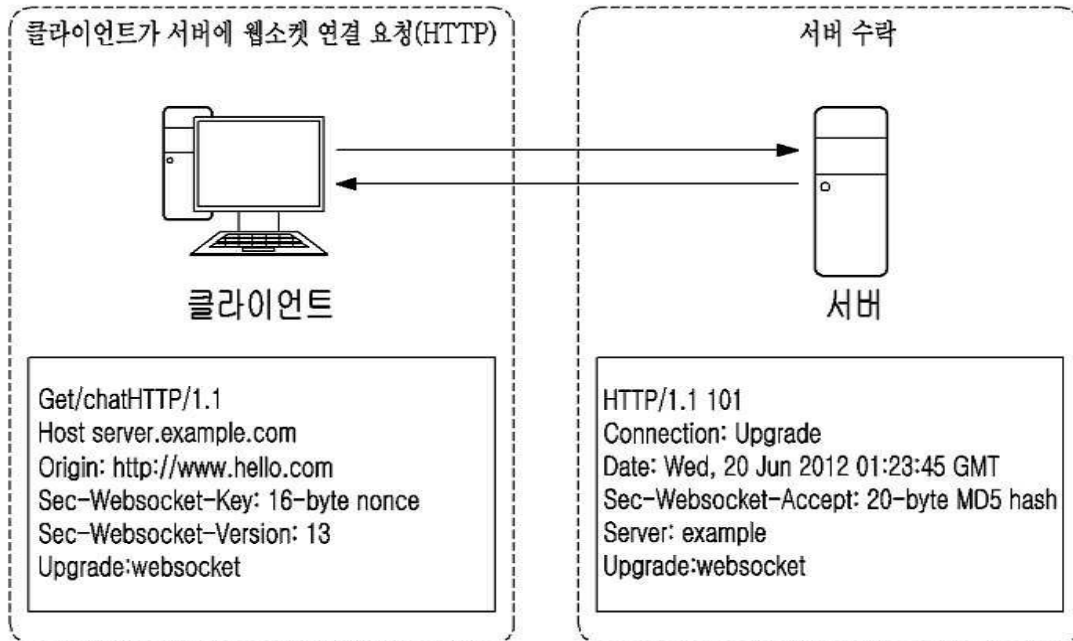


도면2

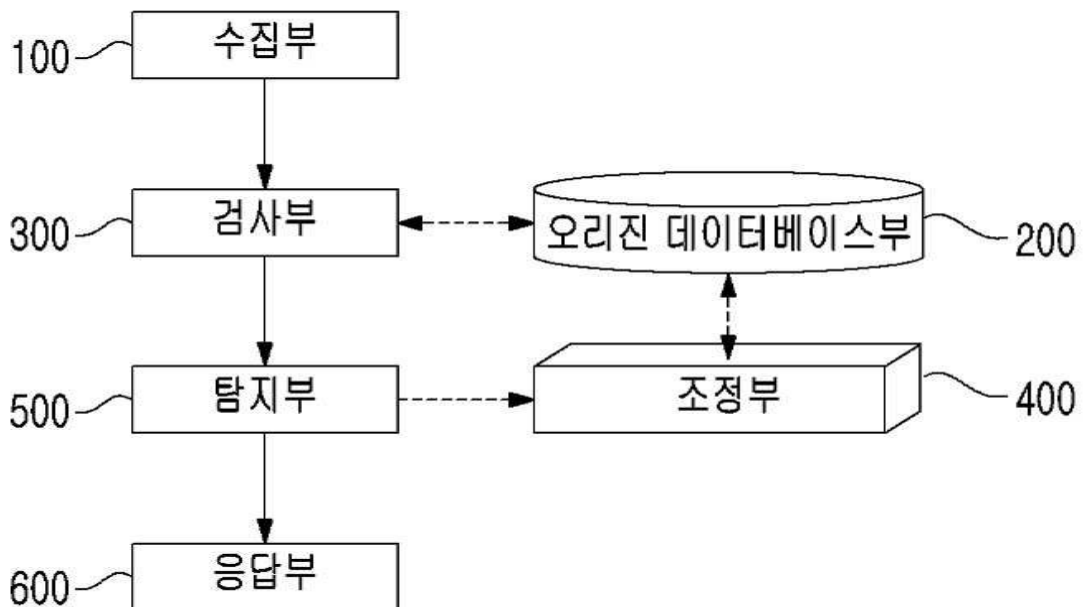
```
Host: echo.websocket.org
Origin: http://websocket.org
Pragma: no-cache
Sec-WebSocket-Extensions: permessage-deflate; client_max_window_bits
Sec-WebSocket-Key: McKW91B1Lqck1wV2lhG5w==
Sec-WebSocket-Version: 13
Upgrade: websocket
```

```
Host: echo.websocket.org
Origin: http://kaazing.org
Pragma: no-cache
Sec-WebSocket-Extensions: permessage-deflate; client_max_window_bits
Sec-WebSocket-Key: DMNi+VY6/c5v1rLQYny8kQ==
Sec-WebSocket-Protocol: kaazing
Sec-WebSocket-Version: 13
Upgrade: websocket
```

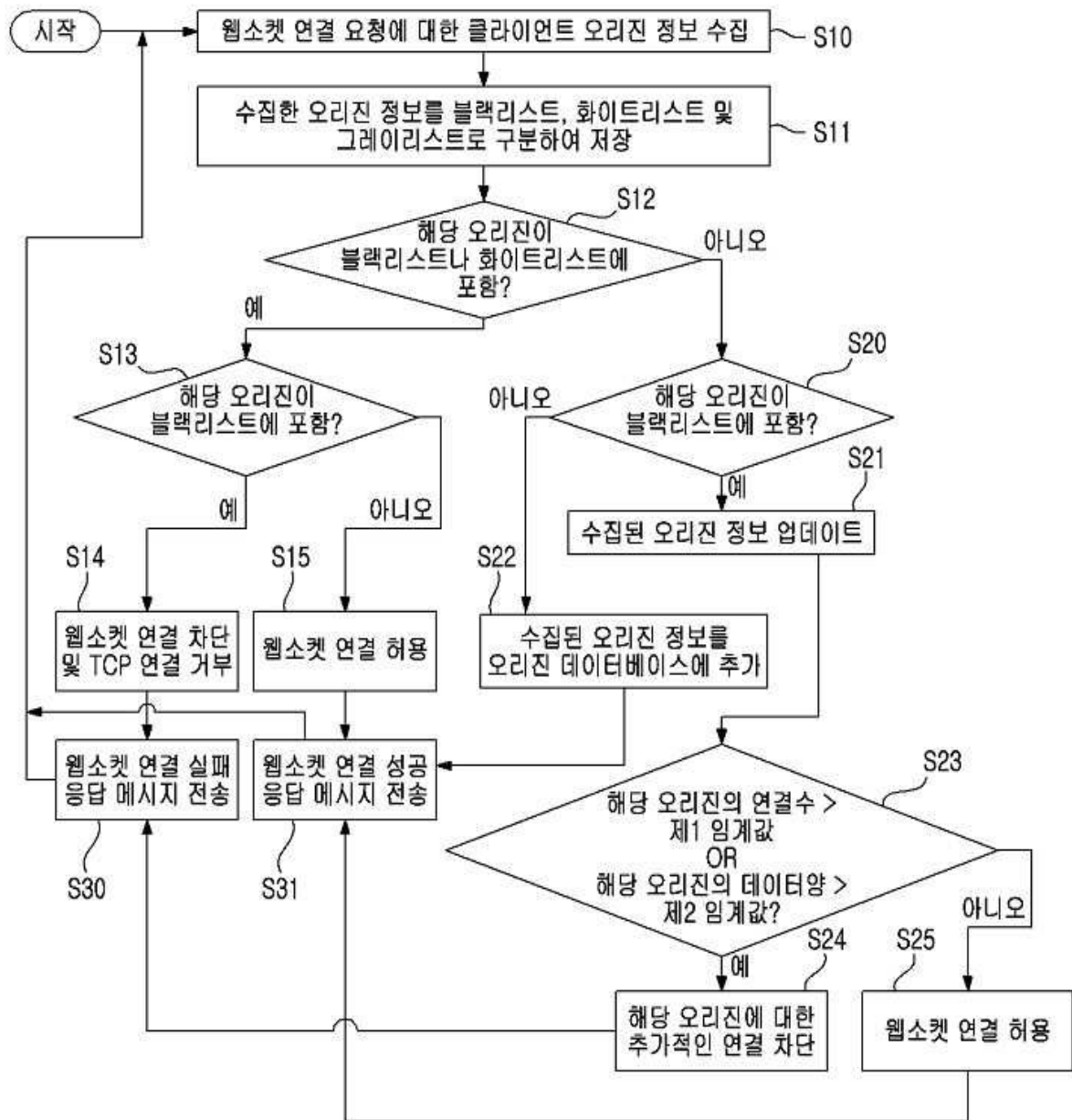
도면3



도면4



도면5



도면6

