(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년05월18일
(11) 등록번호 10-1143368
(24) 등록일자 2012년04월30일

(51) 국제특허분류(Int. Cl.)
H04L 12/22 (2006.01)
(21) 출원번호 10-2010-0121547
(22) 출원일자 2010년12월01일
심사청구일자 2010년12월01일
(56) 선행기술조사문헌
US20050050364 A1*
US6944663 B2
US20100031315 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
양대헌
인천광역시 남구 소성로 71, 하이테크센터 317호 (용현동, 인하대학교)
변제성
인천광역시 남구 소성로 71, 하이테크센터 307호 (용현동, 인하대학교)
(뒷면에 계속)
(74) 대리인
이원희

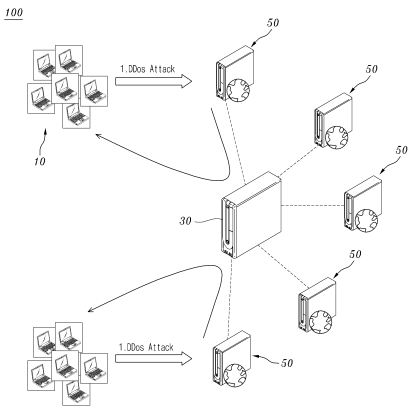
전체 청구항 수 : 총 6 항 심사관 : 양찬호

(54) 발명의 명칭 **분산형 DDos 방어 시스템 및 이를 이용한 방어 방법**

(57) 요 약

분산형 DDos 방어 시스템 및 이를 이용한 방어 방법을 개시한다. 상기 분산형 DDos 방어 시스템은 웹서버로 접근하기 위해 DDos 신호를 웹 서버(50)로 전송하는 사용자 단말기(10) 및 액티브 노드(30)로부터 상기 DDos 신호를 수신하고, 상기 DDos 신호를 송신하는 상기 사용자 단말기(10)의 IP 주소를 탐색하여 상기 사용자 단말기(10)의 상태 정보를 확인하기 위한 비밀 퍼즐 데이터를 상기 사용자 단말기(10)로 전송하는 질의 서버(30), 상기 질의 서버(30)로부터 받은 비밀 퍼즐 데이터의 답의 검증을 수행하는 액티브 노드(35)를 포함한다.

대 표 도 - 도1



(72) 발명자

강전일

인천광역시 남구 소성로 71, 하이테크센터 307호 (용현동, 인하대학교)

맹영재

인천광역시 남구 소성로 71, 하이테크센터 307호 (용현동, 인하대학교)

김성호

인천광역시 남구 소성로 71, 하이테크센터 307호 (용현동, 인하대학교)

신동오

인천광역시 남구 소성로 71, 하이테크센터 307호 (용현동, 인하대학교)

이 발명을 지원한 국가연구개발사업

과제고유번호	41473-01
부처명	IT공과대학
연구사업명	기본연구
연구과제명	인지기반 온라인 금융 서비스와 DDoS 대응 시스템
주관기관	인하대학교 산학협력단
연구기간	2010.05.01 ~ 2013.04.30

특허청구의 범위

청구항 1

웹서버로 접근하기 위해 DDos 신호를 웹 서버(50)로 전송하는 사용자 단말기(10); 및

액티브 노드(35)로부터 상기 DDos 신호를 수신하고, 상기 DDos 신호를 송신하는 상기 사용자 단말기(10)의 IP 주소를 탐색하여 상기 사용자 단말기(10)의 상태 정보를 확인하기 위한 비밀 퍼즐 데이터를 상기 사용자 단말기(10)에 전송하는 질의 서버(30)를 포함하며,

상기 질의 서버(30)는,

상기 DDos 신호를 송신하는 사용자 단말기(10)의 IP 주소를 탐색하여, 탐색된 IP 주소가 접근 가능 IP 인지를 확인하는 액티브 노드(35)를 포함하는 것을 특징으로 하는 분산형 DDos 방버 시스템.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 웹 서버(50)는,

상기 DDos 신호를 송신하는 사용자 단말기(10)의 IP 주소를 탐색하여, 탐색된 IP 주소가 접근 가능 IP 인지를 확인하는 액티브 노드(35)를 포함하는 것을 특징으로 하는 분산형 DDos 방어 시스템.

청구항 4

제1항에 있어서,

상기 액티브 노드(35)는,

상기 질의 서버(30)로부터 전송된 퍼즐 데이터의 응답 여부를 상기 사용자 단말기(10)로부터 수신하여 상기 응답 여부 확인한 후, 상기 사용자 단말기(10)가 상기 웹 서버(50)로의 접근 유무를 가능케 하는 것을 특징으로 하는 분산형 DDos 방어 시스템.

청구항 5

제3항에 있어서,

상기 액티브 노드(35)는,

상기 질의 서버(30)로부터 전송된 퍼즐 데이터의 응답 여부를 상기 사용자 단말기(10)로부터 수신하여 상기 응답 여부 확인한 후, 상기 사용자 단말기(10)가 상기 웹 서버(50)로의 접근 유무를 가능케 하는 것을 특징으로 하는 분산형 DDos 방어 시스템.

청구항 6

웹 서버(50)로 접근하기 위해 사용자 단말기(10)로부터 DDos 신호를 웹 서버(50)로 전송하는 제1단계;

액티브 노드(35)로부터 DDos 신호를 수신하고, 상기 DDos 신호를 송신하는 사용자 단말기(10)의 IP 주소를 탐색하여 상기 사용자 단말기(10)의 상태 정보를 확인하기 위한 비밀 퍼즐 데이터를 질의 서버(30)에서 사용자 단말

기(10)로 전송하는 제2단계; 및

상기 사용자 단말기(10)로부터 상기 비밀 퍼즐 데이터인 암호화 데이터에 상응하는 응답 신호를 상기 액티브 노드(35)에서 수신하여 상기 비밀 퍼즐 데이터 값과 응답 신호인 상기 암호화 데이터 값의 매칭 여부를 확인하는 제3단계를 포함하며,

상기 제2단계는,

상기 웹 서버(50)로부터 DDos 신호를 질의 서버(30)에서 수신하는 a)단계;

상기 질의 서버(30)에서 비밀 퍼즐을 생성하는 b)단계;

상기 액티브 노드(35)로부터 상기 사용자 단말기(10)의 IP 주소 접근 여부를 상기 질의 서버 앞의 액티브 노드에서 확인하는 c)단계; 및

상기 접근 여부에 따라 상기 비밀 퍼즐 데이터의 응답에 상응하는 암호화 데이터를 상기 질의 서버(30)에서 상기 웹 서버(50)를 통해 상기 사용자 단말기(10)로 전송하는 d)단계를 포함하는 분산형 DDos 방어 시스템을 이용한 방어 방법.

청구항 7

삭제

청구항 8

제6항에 있어서,

상기 제3단계는,

상기 비밀 퍼즐 데이터의 데이터 값과 응답 신호의 데이터 값의 매칭 여부에 따라 상기 사용자 단말기(10) 또는 상기 웹 서버(50)로의 접근 유무를 확인하는 단계인 것을 특징으로 하는 분산형 DDos 방어 시스템을 이용한 방어 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 인터넷상에서 서버를 마비시키는 자동화된 봇(좀비 PC, 봇넷)을 통한 DDos 공격에 대응할 수 있는 시스템에 관한 것으로, 보다 상세하게는 자동화된 봇(좀비 PC, 봇넷)은 풀 수 없고 사람만 풀 수 있는 퍼즐을 내는 질의 센터와 자동화된 봇(좀비 PC, 봇넷)과 일반적인 사용자를 구분해주는 액티브 노드(35)로 이루어진 분산형 DDos 방어 시스템 및 이를 이용한 방어 방법에 관한 것이다.

배 경 기 술

[0002] DDos 공격에서 공격자는 대량의 좀비 PC를 보유하고 이를 이용하여 공격하고자 하는 특정 서버로 대량의 트래픽을 전송함으로서, 공격 목적지 경로 상의 라우터, 트래픽, 응용 서비스등을 마비시키는 공격이다.

[0003] 2000년도 초반까지 DDos 공격은 TFN(Tribe Flood Network), TFN2K, Trin00과 같은 공격도구들이나 웜을 통하여 이루어졌다. 당시의 공격은 대량의 트래픽을 발생시키는 유형의 DDos 공격을 수행하기 위한 도구가 설치된 좀비 PC에 공격자가 공격 명령을 내림으로써 수행되었다.

[0004] 이 과정에서 공격자와 좀비 PC는 독자적으로 설계된 통신 프로토콜을 사용하였다. 적은 수의 좀비 PC가 대량의 패킷을 발생시키기 때문에 이러한 공격을 쉽게 탐지가 가능하였다.

[0005] 2000년대 중반에는 DDos 공격에 봇넷과 사회공학적인 공격 방법이 사용되었다. 기존의 DDos 공격과 다르게, 좀

비 PC들은 양산해 내기 위해서 운영체제나 특정 프로그램의 보안 취약점을 이용하는 바이러스나 웜 보다는 전자메일이나 웹 사이트를 이용하였다. 또한 독자적인 통신 프로토콜을 사용하는 것이 아니라 기존에 사용되고 있던 통신 채널을 통하여 좀비 PC에 명령을 전달하는 방식을 취하고 있다.

[0006] 또 공격 대상에 대한 대량의 트래픽이 아니라 특정한 서비스만을 공격하여 패킷의 양을 통한 DDos 공격을 탐지를 어렵게 하였다.

[0007] 2000년대 후반에는 과거와 다르게 고도로 지능화된 DDos 공격이 이루어졌다. 좀비 PC들은 정상적인 범위 안에서 트래픽을 발생하여 기존의 DDos 방어 장비를 무력화하였다.

[0008] 그럼에도 불구하고 대량의 좀비 PC가 사용되어 네트워크의 대역폭을 소전시킬 수 있었다.

[0009] 과거부터 지금까지의 DDos 공격 유형을 살펴보면, 대부분 좀비 PC를 사용한 공통점이 존재한다. 좀비 PC들은 사람의 개입 없이 자동으로 특정 대상을 공격한다.

[0010] 이 특징을 이용하여 사람은 풀기 쉬우나 좀비 PC는 풀기 어려움 퍼즐을 사용자 단말기에게 제공하여, 사람과 좀비 PC를 구분하여 좀비 PC만 서비스에 접근하지 못하도록 함으로써 DDos 공격이 진행 중에 서버의 자원을 보존하고 일반 사용자들은 서비스를 이용하게 할 수 있는 시스템이 필요하다.

[0011]

발명의 내용

해결하려는 과제

[0012] 본 발명이 해결하고자 하는 과제는 사람은 풀기 쉬우나 좀비 PC는 풀기 어려움 퍼즐을 사용자 단말기에게 제공하여, 사람과 좀비 PC를 구분하여 좀비 PC만 서비스에 접근하지 못하도록 함으로써 DDos 공격이 진행 중에 서버의 자원을 보존하고 일반 사용자들은 서비스를 이용하게 할 수 있는 분산형 DDos 방어 시스템을 제공하는 것이다.

과제의 해결 수단

[0013] 상기 과제를 해결하기 위한 본 발명의 실시 예에 따른 분산형 DDos 방어 시스템은 웹서버로 접근하기 위해 DDos 신호를 웹 서버(50)로 전송하는 사용자 단말기(10);

[0014] 상기 웹 서버(50) 앞에서 상기 DDos 신호를 감지하고, 상기 DDos 신호를 송신하는 상기 사용자 단말기(10)의 IP 주소를 탐색하여 상기 DDos 신호를 상기 징의 서버(30)로 보내주는 상기 액티브 노드(35); 및

[0015] 상기 웹 서버(50) 앞의 상기 액티브 노드(35)로부터 상기 DDos 신호를 수신하고, 상기 DDos 신호를 송신하는 상기 사용자 단말기(10)의 IP 주소를 탐색하여 상기 사용자 단말기(10)의 상태 정보를 확인하기 위한 비밀 퍼즐 데이터를 상기 사용자 단말기(10)로 전송하는 질의 서버를 포함한다.

[0016] 상기 질의 서버(30)는 상기 DDos 신호를 송신하는 사용자 단말기(10)의 IP 주소를 탐색하여, 비밀 퍼즐 데이터 제공 횟수를 확인하는 액티브 노드(35)를 포함하는 것을 특징으로 한다.

[0017] 상기 웹 서버(50)는 상기 DDos 신호를 송신하는 사용자 단말기(10)의 IP 주소를 탐색하여, 탐색된 IP 주소가 접근 가능 IP 인지를 확인하는 액티브 노드(35)를 포함하는 것을 특징으로 한다.

[0018] 상기 액티브 노드(35)는 상기 질의 서버(30)로부터 전송된 퍼즐 데이터의 응답 여부를 상기 사용자 단말기(10)로부터 수신하여 상기 응답 여부 확인한 후, 상기 사용자 단말기(10)가 상기 웹 서버(50)로의 접근 유무를 가능케 하는 것을 특징으로 한다.

[0019] 상기 액티브 노드(35)는 상기 질의 서버(30)로부터 전송된 퍼즐 데이터의 응답 여부를 상기 사용자 단말기(10)로부터 수신하여 상기 응답 여부 확인한 후, 상기 사용자 단말기(10)가 상기 웹 서버(50)로의 접근 유무를 가능케 하는 것을 특징으로 한다.

[0020] 상기 질의 서버(30)에 포함되어 있는 액티브 노드(35)는 상기 사용자 단말기(10)에 비밀 퍼즐 데이터를 제공하는 횟수를 기록하고, 임계치를 초과할 경우 사용자 단말기(10)를 좀비 PC로 간주하고, 상기 서버(30)에 접근을 못하도록 하는 것을 특징으로 한다.

[0021] 상기 과제를 해결하기 위한 본 발명의 실시 예에 따른 분산형 DDos 방어 시스템을 이용한 방어 방법은 웹 서버(50)로 접근하기 위해 사용자 단말기(10)로부터 DDos 신호를 웹 서버(50)로 전송하는 제1단계, 상기 웹 서버(50)로부터 DDos 신호를 수신하고, 상기 DDos 신호를 송신하는 사용자 단말기(10)의 IP 주소를 탐색하여 상기 사용자 단말기(10)의 상태 정보를 확인하기 위한 비밀 퍼즐 데이터를 상기 웹 서버(50)를 통해 질의 서버(30)에서 사용자 단말기(10)로 전송하는 제2단계 및 상기 사용자 단말기(10)로부터 상기 비밀 퍼즐 데이터인 암호화 데이터에 상응하는 응답 신호를 상기 액티브 노드(35)에서 수신하여 상기 비밀 퍼즐 데이터 값과 응답 신호인 상기 암호화 데이터 값의 매칭 여부를 확인하는 제3단계를 포함한다.

[0022] 상기 제2단계는 상기 액티브 노드(35)로부터 DDos 신호를 질의 서버(30)에서 수신하는 a)단계, 상기 질의 서버(30)에서 비밀 퍼즐을 생성하는 b)단계, 상기 질의 서버(30)가 생성한 비밀 퍼즐을 전송하는 c)단계, 상기 사용자 단말기(10)가 상기 질의 서버(30)로부터 받은 비밀 퍼즐의 답을 상기 액티브 노드(35)에게 답을 전송하는 d)단계, 상기 사용자 단말기(10)로부터 받은 비밀 퍼즐의 답을 검증하여 상기 사용자 단말기(10)의 IP 주소 접근 여부를 상기 액티브 노드(35)에서 확인하는 f)단계를 포함하는 것을 특징으로 한다.

[0023] 상기 제3단계는 상기 비밀 퍼즐 데이터의 데이터 값과 응답 신호의 데이터 값의 매칭 여부에 따라 상기 사용자 단말기(10)의 상기 웹 서버(50)로의 접근 유무를 확인하는 단계인 것을 특징으로 한다.

발명의 효과

[0024] 본 발명에 따르면, 분산형 DDos 공격에 대응하기 위해 분산형 DDos 방어 시스템을 구축함으로써 좀비 PC로 부터 오는 데이터를 막아줄 수 있어, 웹서버의 부하를 줄일 수 있으며, 그에 따른 안전한 DDos 공격을 막을 수 있는 효과가 있다.

도면의 간단한 설명

[0025] 도 1은 본 발명의 실시 예에 따른 분산형 DDos 방어 시스템을 나타낸 블럭도이다.

도 2는 본 발명의 실시 예에 따른 분산형 DDos 방어 시스템에서 사용자 단말기(10)의 인증 과정을 설명하기 위한 예시도이다.

도 3은 도 2에 도시된 제2단계를 보다 상세하게 설명하기 위한 예시도이다.

도 4는 도 2에 도시된 제3단계를 보다 상세하게 설명하기 위한 예시도이다.

발명을 실시하기 위한 구체적인 내용

[0026] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시 예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 여기에서 설명하는 실시 예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기

위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0027] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "~부","~기" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0028] 본 발명과 본 발명의 동작상의 이점 및 본 발명의 실시에 의하여 달성되는 목적을 충분히 이해하기 위해서는 본 발명의 바람직한 실시 예를 예시하는 첨부 도면 및 도면에 기재된 내용을 참조하여야 한다.

[0029] 이하, 첨부된 도면을 참조하여 본 발명의 구체적인 내용을 설명하도록 한다.

[0030] 도 1은 본 발명의 실시 예에 따른 분산형 DDos 방어 시스템을 나타낸 블럭도이다.

[0031] 도 1에 도시된 바와 같이, 본 발명의 DDos 방어 시스템은 사용자 단말기(10), 웹 서버(50) 및 질의 서버(30)를 포함한다.

[0032] 상기 액티브 노드(35)는 외부로부터 유입되는 DDos 어택을 감지하여 그에 따른 감지 신호를 센싱하여 상기 질의 서버(30)로 전송한다.

[0033] 상기 질의 서버(30)는 상기 액티브 노드(35)로부터 상기 사용자 단말기(10)로부터 전송된 감지 신호를 수신하고, 상기 DDos 어택을 송신한 사용자 단말기(10)의 IP 주소를 탐색하여 상기 사용자 단말기(10)의 상태 정보를 확인하기 위한 비밀 퍼즐 데이터를 상기 사용자 단말기(10)로 전송한다.

[0034] 보다 구체적으로, 상기 질의 서버(30)는 상기 DDos 어택의 사용자 단말기(10)의 IP 주소를 탐색하여, 탐색된 IP 주소가 퍼즐 제공 횟수를 초과하였는지 확인하는 액티브 노드(35)를 포함한다.

[0035] 상기 웹 서버(50)는 상기 DDos 어택의 사용자 단말기(10)의 IP 주소를 탐색하여, 탐색된 IP 주소가 접근 가능 IP 인지를 확인하는 액티브 노드(35)를 포함한다.

[0036] 여기서, 상기 액티브 노드(35)는 상기 질의 서버(30)로부터 전송된 퍼즐 데이터의 응답 여부를 상기 사용자 단말기(10)로부터 수신하여 상기 응답 여부를 확인한 후, 상기 사용자 단말기(10)가 상기 웹 서버(50)로의 접근 유무를 가능케 하도록 수행하는 역할을 한다.

[0037] 도 2는 본 발명의 실시 예에 따른 분산형 DDos 방어 시스템에서 사용자 단말기(10)의 인증 과정을 설명하기 위한 예시도이다.

[0038] 도 2를 참조하면, 본 발명의 분산형 DDos 방어 시스템을 이용한 사용자 단말기(10)의 인증과정은 제1단계 내지 제3단계를 포함한다.

[0039] 상기 제1단계는 웹 서버(50)로 접근하기 위해 사용자 단말기(10)로부터 DDos 신호를 웹 서버(50)로 전송하는 단계(1st)일 수 있다.

[0040] 상기 제2단계는 상기 액티브 노드(35)가 DDos 신호를 수신하는 단계(2st), 상기 DDos 신호를 송신하는 사용자 단말기(10)의 IP 주소를 탐색하여 상기 사용자 단말기(10)의 상태 정보를 확인하기 위해 상기 DDos 신호를 상기 질의 서버(30)로 전송한 후, 상기 질의 서버에서 생성된 비밀 퍼즐 데이터를 상기 사용자 단말기(10)로 전송하는 단계(3st)를 포함한다.

[0041] 상기 제3단계는 상기 사용자 단말기(10)로부터 상기 비밀 퍼즐 데이터인 암호화 데이터에 상응하는 응답 신호를

상기 액티브 노드(35)에서 수신하는 단계(4st)와 상기 비밀 퍼즐 데이터 값과 응답 신호인 상기 암호화 데이터 값의 매칭 여부를 액티브 노드(35)에서 확인하여 상기 웹 서버(50)에게 데이터를 전송하는 단계(5st)를 포함한다.

[0042] 보다 구체적으로, 상기 제2단계는 상기 사용자 단말기(10)로부터 DDos 신호를 상기 액티브 노드(35)에서 수신한다. 이때, 상기 액티브 노드가 상기 질의 서버로 DDos 신호를 전송시, 상기 질의 서버 앞의 액티브 노드(35)는 상기 사용자 단말기(10)의 IP가 비밀 퍼즐 데이터를 받은 횟수를 확인 후, 받은 횟수가 임계치를 넘을 경우 해당 패킷을 버리고, 넘지 않은 경우 비밀 퍼즐 데이터를 상기 사용자 단말기로 전송한다.

[0043] 만약, 상기 화이트 리스트에 상기 사용자 단말기(10)의 IP 주소가 있을 경우, 상기 사용자가 단말기(10)로부터 받은 신호를 상기 웹 서버(50)로 바로 전송한다. 그러나, 상기 화이트 리스트에 상기 사용자 단말기(10)의 IP 주소가 없고 블랙 리스트에 없는 경우, 상기 액티브 노드(35)는 상기 DDos 신호를 상기 질의 서버(30)로 재전송한다. 마지막으로 상기 사용자 단말기(10)의 IP 주소가 블랙 리스트에 있는 경우, 액티브 노드(35)는 상기 DDos 신호를 폐기한다.

[0044] 다음으로, 질의 서버(30)는 DDos 신호를 수신하여 상기 DDos 신호를 송신한 사용자 단말기(10)가 좀비 PC 인지의 상태 확인을 위한 암호화된 비밀 퍼즐 데이터를 사용자 단말기(10)로 전송한다.

[0045] 상기 제3단계는 상기 사용자 단말기(10)로부터 상기 비밀 퍼즐 데이터인 암호화 데이터에 상응하는 응답 신호를 상기 웹 서버 내의 액티브 노드(35)에서 수신(4st)한 후, 상기 비밀 퍼즐 데이터 값과 응답 신호인 상기 암호화 데이터 값의 매칭 여부를 액티브 노드(35)에서 확인한다.

[0046] 상기 웹 서버 내의 액티브 노드(35)는 매칭 여부 확인 후 값이 올바른 경우 해당 상기 사용자 단말기(10)의 IP를 상기 화이트리스트에 재등록하게 된다. IP가 등록된 사용자 단말기(10)는 위에 언급한 절차를 거칠 필요없이 상기 웹 서버의 자원에 접근하게 된다.

[0047] 도 3은 도 2에 도시된 제2단계를 보다 상세하게 설명하기 위한 예시도이며, 도 4는 도 2에 도시된 제3단계를 보다 상세하게 설명하기 위한 예시도이다.

[0048] 도 3 및 도 4에 도시된 바와같이, 상기 질의 서버(30)는 미리 비밀 퍼즐을 생성하고 있다가, 액티브 노드(35)로부터 HTTP Redirect를 먼저 받으면 사용자 단말기(10)의 IP가 질의 서버의 블랙 리스트에 있는지 확인 후, 세션키를 퍼즐의 답을 암호화한 C1과 세션키 S와 사용자 단말기(10)의 IP와 타임스탬프 t를 서버와 액티브 노드(35) 사이의 공유키로 암호화한 C2를 퍼즐과 함께 사용자 단말기(10)로 전송한다.

[0049] 상기 사용자 단말기(10)는 질의 서버(30)로부터 퍼즐과 C1과 C2를 받으면 퍼즐을 푼 후 퍼즐의 답으로 C_1을 복호화하여 세션키 S을 찾아낸다.

[0050] 사용자 단말기(10)는 복사 공격을 방지하기 위해 N(Nonce)을 생성한 후, N에 $N+C_2$를 붙인 후 세션키 S'으로 암호화하여 V를 생성한 후 V와 C2를 액티브 노드(35)에 전송한다.

[0051] 상기 액티브 노드(35)는 사용자 단말기(10)로부터 V와 C_2를 받으면 C_2를 질의 센터와 액티브 노드(35) 사이의 공유키 SK로 복호화하여 세션키 S와 사용자 단말기(10)의 IP와 타임스탬프 t를 복원한다. 상기 V를 세션키 S로 복호화하여 N'과 O(N+C2)를 복원한 후, N'과 C_2를 Xor 연산한 값이 O값과 같다면 사용자 단말기(10)는 퍼즐을 올바르게 풀었기 때문에 화이트 리스트에 추가하고, 퍼즐에 대한 답이 틀린 경우에는 블랙 리스트에 추가한다.

[0052] 따라서, 본 발명은 DDos 공격이 진행 중일 때 액티브 노드(35)는 사용자 단말기(10)의 IP가 화이트리스트(White list)에 있는지 확인한다.

[0053] 화이트리스트에 있을 경우, 패킷을 웹 서버(50)로 바로 전송해 주고, 블랙리스트에 있는 경우에는 해당 패킷을 폐기하고, 블랙 리스트에 없고 HTTP Request에 퍼즐의 답이 들어있는 패킷이 아닌 경우에는 HTTP Request를 질의 센터로 재전송한다.

[0054] 상기 질의 센터는 사용자 단말기(10)가 사용자인지 좀비 PC 인지 구별하기 위한 비밀 퍼즐을 사용자 단말기(10)로 전송하고, 상기 사용자 단말기(10)는 비밀 퍼즐을 푼 후 그 값을 액티브 노드(35)에게 전송해주면 액티브 노드(35)는 값을 확인 후 값이 올바른 경우 해당 IP를 화이트 리스트에 등록한 후 웹 서버(50)로 패킷을 전송해 준다. 만약 틀린 경우에는 블랙 리스트에 등록한다.

[0055] 한번 인증이 완료된 사용자 단말기(10)의 IP는 화이트 리스트에 모두 등록되어 있기 때문에, 퍼즐을 다시 풀 필요가 없이 바로 웹 서버(50)의 자원에 접근할 수 있다.

[0056] 따라서, 본 발명에 따른 DDos 공격에 대응하기 위해 분산형 DDos 방어 시스템을 구축함으로써 서버를 안전하게 유지시킬 수 있고, 웹서버 운영자는 웹서버 앞에 액티브 노드(35)만 설치해 주면, 액티브 노드(35)가 질의 서버와 연동하여 좀비 PC로부터 오는 데이터를 막아주기 때문에 웹 서버의 부하 없이 안전하게 DDos 공격을 막을 수 있다.

[0057] 대부분 좀비 PC의 경우에는 사람의 개입 없이 스스로 질의 서버가 내는 퍼즐을 풀 수 없으므로 DDos 공격에 대해서 안전하리라 예상된다.

[0058] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

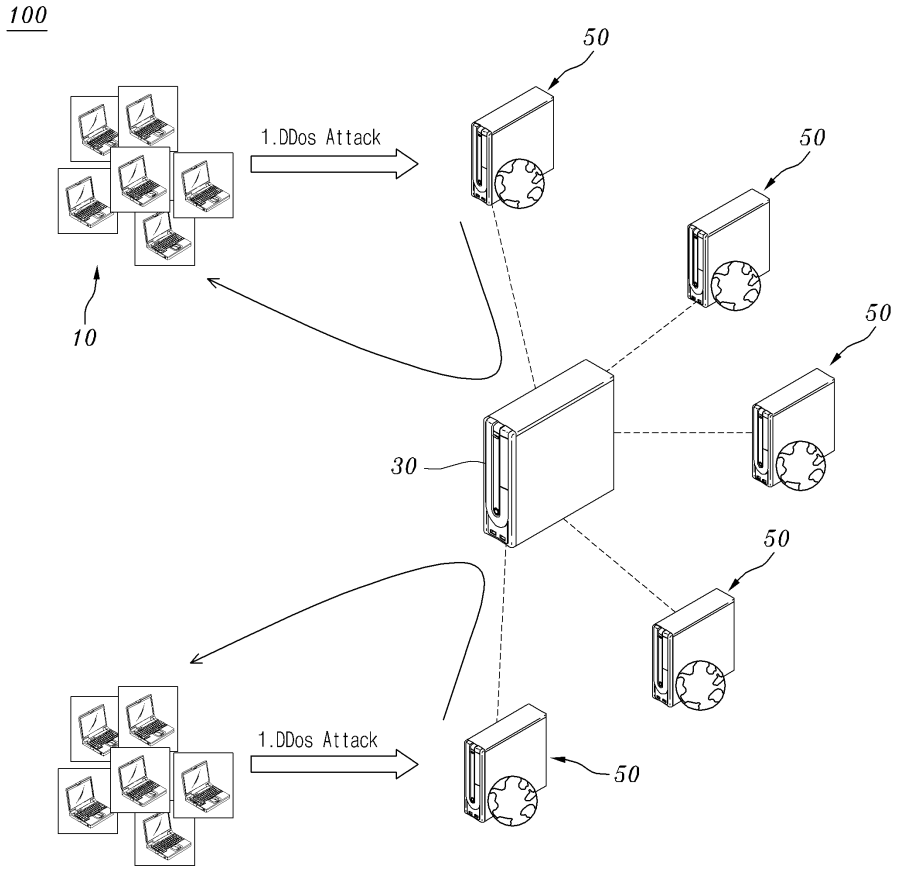
부호의 설명

[0059] 10: 사용자 단말기 30: 질의 서버

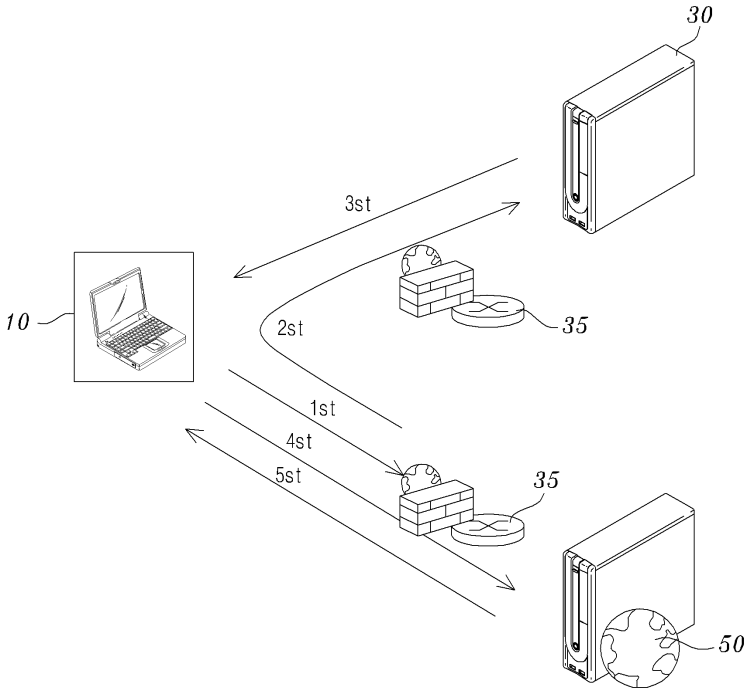
35: 액티브 노드 50: 웹 서버

도면

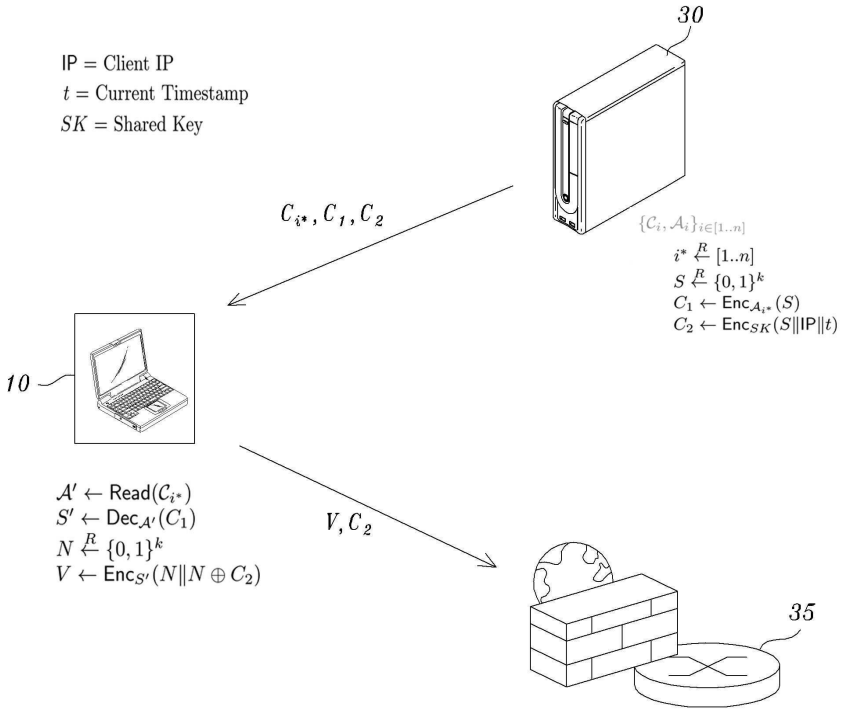
도면1



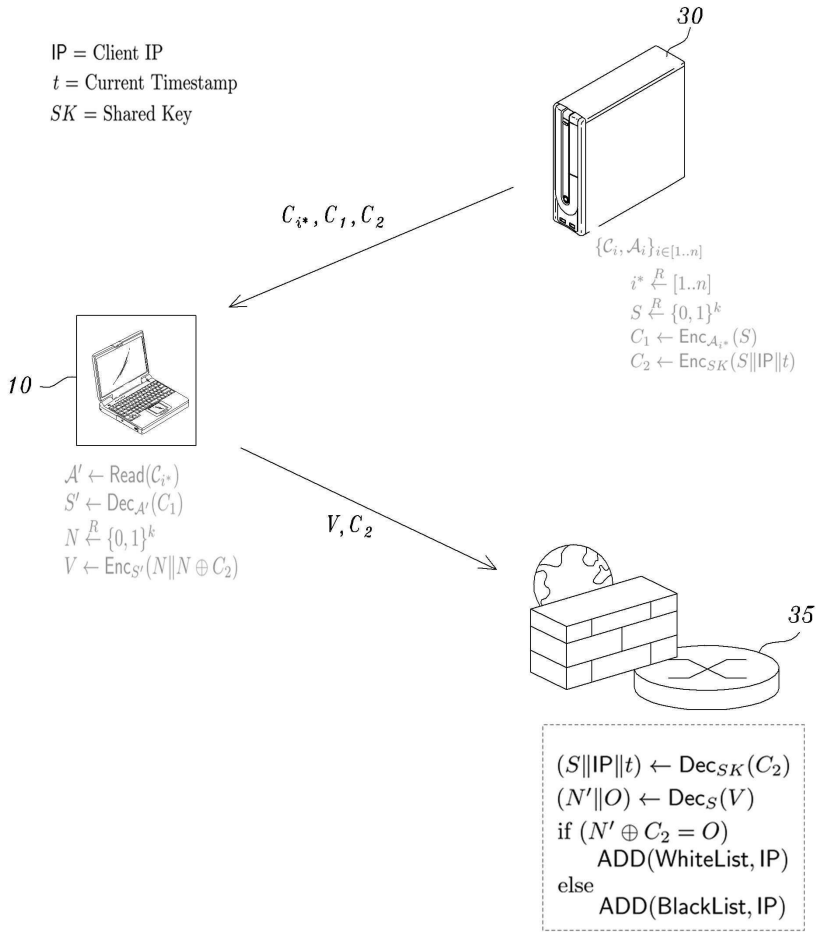
도면2


30
3st
10
35
2st
1st
4st
5st
35
50

도면3


IP = Client IP
t = Current Timestamp
SK = Shared Key
30
C_{i^*}, C_1, C_2
$\{C_i, \mathcal{A}_i\}_{i\in[1..n]}$
$i^* \xleftarrow{R} [1..n]$
$S \xleftarrow{R} \{0,1\}^k$
$C_1 \leftarrow \mathsf{Enc}_{\mathcal{A}_{i^*}}(S)$
$C_2 \leftarrow \mathsf{Enc}_{SK}(S\|\mathsf{IP}\|t)$
10
$\mathcal{A}' \leftarrow \mathsf{Read}(\mathcal{C}_{i^*})$
$S' \leftarrow \mathsf{Dec}_{\mathcal{A}'}(C_1)$
$N \xleftarrow{R} \{0,1\}^k$
$V \leftarrow \mathsf{Enc}_{S'}(N\|N \oplus C_2)$
V, C_2
35

도면4


IP = Client IP
t = Current Timestamp
SK = Shared Key
30
C_{i^*}, C_1, C_2
$\{\mathcal{C}_i, \mathcal{A}_i\}_{i\in[1..n]}$
$i^* \xleftarrow{R} [1..n]$
$S \xleftarrow{R} \{0,1\}^k$
$C_1 \leftarrow \mathsf{Enc}_{\mathcal{A}_{i^*}}(S)$
$C_2 \leftarrow \mathsf{Enc}_{SK}(S\|\mathsf{IP}\|t)$
10
$\mathcal{A}' \leftarrow \mathsf{Read}(\mathcal{C}_{i^*})$
$S' \leftarrow \mathsf{Dec}_{\mathcal{A}'}(C_1)$
$N \xleftarrow{R} \{0,1\}^k$
$V \leftarrow \mathsf{Enc}_{S'}(N\|N \oplus C_2)$
V, C_2
35
$(S\|\mathsf{IP}\|t) \leftarrow \mathsf{Dec}_{SK}(C_2)$
$(N'\|O) \leftarrow \mathsf{Dec}_S(V)$
if $(N' \oplus C_2 = O)$
ADD(WhiteList, IP)
else
ADD(BlackList, IP)