(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2012 년 6 월 21 일 (21.06.2012)

WIPO | PCT

(10) 국제공개번호
WO 2012/081903 A1

(51) 국제특허분류:
H04L 12/22 (2006.01)

(21) 국제출원번호: PCT/KR2011/009619

(22) 국제출원일: 2011 년 12 월 14 일 (14.12.2011)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2010-0127821 2010 년 12 월 14 일 (14.12.2010) KR

(71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): **한국전자통신연구원 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE)** [KR/KR]; 대전광역시 유성구 가정동 161 번지, 305-350 Daejeon (KR).

(72) 발명자; 겸
(75) 발명자/출원인 (US 에 한하여): **김병구 (KIM, Byoung-Koo)** [KR/KR]; 대전광역시 유성구 반석동 반석마을아파트 609-1602, 305-750 Daejeon (KR). **윤승용 (YOON, Seung-Yong)** [KR/KR]; 대전광역시 서구 도마 2 동 경남아파트 116-1006, 302-763 Daejeon (KR).

(74) 대리인: **한양특허법인 (HANYANG PATENT FIRM)**; 서울특별시 강남구 도곡동 412-1 한양빌딩, 135-854 Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

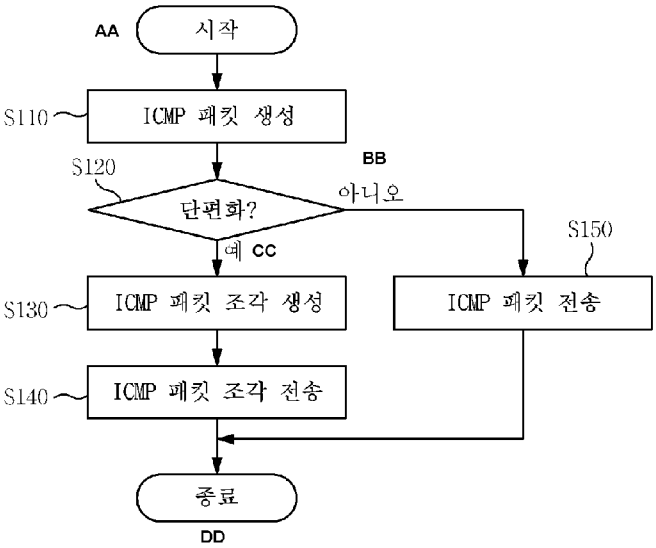
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG,

[다음 쪽 계속]

(54) **Title**: METHOD FOR BLOCKING A DENIAL-OF-SERVICE ATTACK

(54) **발명의 명칭** : 서비스 거부 공격 차단 방법

[Fig. 2]



AA ... Start
BB ... No
CC ... Yes
DD ... End
S110 ... Generating an ICMP packet
S120 ... Fragmentizing?
S130 ... Generating ICMP packet fragments
S140 ... Transmitting ICMP packet fragments
S150 ... Transmitting the ICMP packet

(57) **Abstract**: A server receives a first echo request message which complies with an Internet control message protocol, extracts filtering information from header information of the received first echo request message, and when a second echo request message which complies with the Internet control message protocol is received, compares header information of the received second echo request message and the extracted filtering information so as to determine whether to block an attacking packet for the received second echo request message. According to the present invention, the server blocks the attacking packet using the Internet control message protocol, thereby blocking a denial-of-service attack.

(57) **요약서**: 서버는 인터넷 제어 메시지 프로토콜을 따르는 제 1 반향 요청 메시지를 수신하고, 수신된 제 1 반향 요청 메시지의 헤더 정보에서 필터링 정보를 추출하며, 이후에 인터넷 제어 메시지 프로토콜을 따르는 제 2 반향 요청 메시지가 수신되면, 수신된 제 2 반향 요청 메시지의 헤더 정보와 추출된 필터링 정보를 비교하여 수신된 제 2 반향 요청 메시지에 대한 공격 패킷 여부를 결정한다. 이를 통해 서버는 인터넷 제어 메시지 프로토콜을 이용한 공격 패킷을 차단함으로써, 서비스 거부 공격을 차단한다.

WO 2012/081903 A1

ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

규칙 4.17에 의한 선언서:

— 특허출원 및 특허를 받을 수 있는 출원인의 자격에 관한 선언 (규칙 4.17(ii))

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

명세서

발명의 명칭: 서비스 거부 공격 차단 방법

기술분야

[1] 본 발명은 서비스 거부 공격을 차단하는 방법(method for blocking denial-of-service attack)에 관한 것이다. 보다 상세하게, 본 발명은 ICMP 플러딩에 의한 서비스 거부 공격을 차단하는 방법에 관한 것이다.

[2] 본 발명은 2010년 12월 14일 출원된 한국특허출원 제10-2010-0127821호의 출원일의 이익을 주장하며, 그 내용 전부는 본 명세서에 포함된다.

배경기술

[3] 서비스 거부 공격(Denial-of-Service attack, 이하에서는 'DoS 공격'이라고도 함)은 웹 사이트(web site)나 도메인 네임 서버(Domain Name Server) 등을 대상으로 하여 네트워크나 서버의 이용도(availability)를 저하시킨다. 특히, 분산 서비스 거부 공격(Distributed Denial of Service attack, 이하에서는 'DDoS 공격'이라고도 함)은 악성코드에 감염된 다수의 좀비 컴퓨터(zombie computer)에서 동시에 DoS 공격을 수행하는 방식이다.

[4] 여기서, 인터넷 제어 메시지 프로토콜(Internet Control Message Protocol, 이하에서는 'ICMP'이라고도 함)은 호스트와 호스트, 또는 호스트와 라우터간의 에러 상태 또는 상태 변화를 알려주고 요청에 대해 응답하는 기능을 제공하는 프로토콜로써, 활성화된 서비스나 포트가 필요하지 않다는 특징을 가진다.

[5] 이때, DDoS 공격 중 ICMP 플러딩(ICMP Flooding)은 인터넷 제어 메시지 프로토콜(ICMP)의 특징을 악용하여 대량의 ICMP 패킷을 공격 대상에게 전달하는 방식으로 수행된다.

[6] 하지만, 종래의 공격 탐지 및 대응 기법들은 정상적인 사용자와 악의적인 사용자의 행위를 구별하는 것이 쉽지 않고, 트래픽 측정에 의한 일률적인 차단은 정상적인 사용자의 트래픽까지 차단하는 문제점이 있다. 따라서, 정상적인 사용자의 트래픽은 보호하면서 악의적인 사용자에 의한 공격 트래픽만을 선별하여 차단하는 기법이 필요하다.

발명의 상세한 설명

기술적 과제

[7] 본 발명은 상기한 바와 같은 문제점을 해결하기 위하여 제안된 것으로써, 공격 트래픽의 형태별 특성에 따른 서비스 거부 공격 특히, ICMP 플러딩 공격을 차단하는 방법을 제공하기 위한 것이다.

과제 해결 수단

[8] 본 발명의 특징에 따른 서비스 거부 공격 차단 방법은 서버가 인터넷 제어 메시지 프로토콜을 이용한 공격 패킷을 차단하는 서비스 거부 공격 차단 방법으로써, 인터넷 제어 메시지 프로토콜을 따르는 제1 반향 요청 메시지를

수신하는 단계, 제1 반향 요청 메시지의 헤더 정보에서 필터링 정보를 추출하는 단계, 인터넷 제어 메시지 프로토콜을 따르는 제2 반향 요청 메시지를 수신하는 단계, 그리고 제2 반향 요청 메시지의 헤더 정보와 필터링 정보를 비교하여 제2 반향 요청 메시지에 대한 공격 패킷 여부를 결정하는 단계를 포함한다.

[9] 본 발명의 다른 특징에 따른 서비스 거부 공격 차단 방법은 서버가 인터넷 제어 메시지 프로토콜을 이용한 공격 패킷을 차단하는 서비스 거부 공격 차단 방법으로써, 수신된 복수 개의 패킷들 각각의 헤더 정보를 이용하여 복수 개의 패킷들 중에서 의심 패킷을 추출하는 단계, 의심 패킷의 헤더 정보에서 필터링 정보를 추출하는 단계, 인터넷 제어 메시지 프로토콜을 따르는 메시지를 수신하는 단계, 그리고 필터링 정보와 메시지의 헤더 정보를 비교하여 메시지에 대한 공격 패킷 여부를 결정하는 단계를 포함한다.

발명의 효과

[10] 본 발명에 따르면 다음과 같은 효과를 기대할 수 있다. ICMP 플러딩의 공격 형태를 분류하고, 각 형태별 특성에 따른 공격 패킷의 탐지 및 차단 방법을 제공함으로써, 다양한 형태의 ICMP 플러딩에 대해 악의적인 사용자의 행위만을 차단하여 정상적인 사용자에게 원활한 네트워크 서비스를 제공할 수 있다.

도면의 간단한 설명

[11] 도 1은 본 발명의 실시 예에 따른 클라이언트 서버 시스템의 구성을 도시한 도면이다.

[12] 도 2는 본 발명의 제1 실시 예에 따른 공격 패킷 전송 방법을 도시한 도면이다.

[13] 도 3은 본 발명의 실시 예에 따른 ICMP 패킷의 구조를 도시한 도면이다.

[14] 도 4는 본 발명의 실시 예에 따른 ICMP 패킷에 포함된 IP 헤더의 구조를 도시한 도면이다.

[15] 도 5는 본 발명의 실시 예에 따른 ICMP 패킷에 포함된 ICMP 헤더의 구조를 도시한 도면이다.

[16] 도 6은 본 발명의 실시 예에 따른 단편화된 ICMP 패킷의 구조를 도시한 도면이다.

[17] 도 7은 본 발명의 실시 예에 따른 ICMP 패킷 조각에 포함된 IP 헤더의 구조를 도시한 도면이다.

[18] 도 8은 본 발명의 실시 예에 따른 ICMP 패킷 조각에 포함된 ICMP 헤더의 구조를 도시한 도면이다.

[19] 도 9는 본 발명의 제1 실시 예에 따른 서버가 서비스 거부 공격을 차단하는 방법을 도시한 도면이다.

[20] 도 10은 본 발명의 제1 실시 예의 하나의 예에 따른 서버가 공격 패킷을 탐지하는 방법을 도시한 도면이다.

[21] 도 11은 본 발명의 제1 실시 예의 다른 예에 따른 서버가 공격 패킷을 탐지하는 방법을 도시한 도면이다.

[22] 도 12는 본 발명의 제2 실시 예에 따른 서버가 서비스 거부 공격을 차단하는 방법을 도시한 도면이다.

[23] 도 13은 본 발명의 제2 실시 예의 하나의 예에 따른 서버가 공격 패킷을 탐지하는 방법을 도시한 도면이다.

[24] 도 14는 본 발명의 제2 실시 예의 다른 예에 따른 서버가 공격 패킷을 탐지하는 방법을 도시한 도면이다.

[25] 도 15는 본 발명의 제3 실시 예에 따른 서버가 서비스 거부 공격을 차단하는 방법을 도시한 도면이다.

[26] 도 16은 본 발명의 제2 실시 예에 따른 공격 패킷 전송 방법을 도시한 도면이다.

[27] 도 17은 본 발명의 실시 예에 따른 ICMP 질의 메시지의 구조를 도시한 도면이다.

[28] 도 18은 본 발명의 실시 예에 따른 ICMP 질의 메시지에 포함된 IP 헤더의 구조를 도시한 도면이다.

[29] 도 19는 본 발명의 실시 예에 따른 ICMP 질의 메시지에 포함된 ICMP 헤더의 구조를 도시한 도면이다.

[30] 도 20은 본 발명의 제4 실시 예에 따른 서버가 서비스 거부 공격을 차단하는 방법을 도시한 도면이다.

[31] 도 21은 본 발명의 제4 실시 예의 하나의 예에 따른 서버가 공격 패킷을 탐지하는 방법을 도시한 도면이다.

[32] 도 22는 본 발명의 제4 실시 예의 다른 예에 따른 서버가 공격 패킷을 탐지하는 방법을 도시한 도면이다.

[33] 도 23은 본 발명의 제4 실시 예의 또 다른 예에 따른 서버가 공격 패킷을 탐지하는 방법을 도시한 도면이다.

발명의 실시를 위한 형태

[34] 본 발명을 첨부된 도면을 참고하여 상세히 설명하면 다음과 같다. 여기서, 반복되는 설명, 본 발명의 요지를 불필요하게 흐릴 수 있는 고지 기능, 및 구성에 대한 상세한 설명은 생략한다. 본 발명의 실시형태는 당 업계에서 평균적인 지식을 가진 자에게 본 발명을 보다 완전하게 설명하기 위해서 제공되는 것이다. 따라서, 도면에서의 요소들의 형상 및 크기 등은 보다 명확한 설명을 위해 과장될 수 있다.

[35] 이제 도면을 참고하여 본 발명의 실시 예에 따른 서비스 거부 공격 차단 방법에 대해 설명한다.

[36] 먼저, 도 1을 참고하여 본 발명의 실시 예에 따른 클라이언트 서버 시스템(client-server system)에 대해 설명한다.

[37] 도 1은 본 발명의 실시 예에 따른 클라이언트 서버 시스템의 구성을 도시한 도면이다.

[38] 도 1에 도시된 바와 같이, 클라이언트 서버 시스템은 복수 개의

클라이언트(100) 및 서버(200)를 포함한다.

[39] 클라이언트(100)는 서버(200)와 연결하여 주된 작업이나 정보를 서버(200)에게 요청하고 그 결과를 돌려받는다.

[40] 서버(200)는 클라이언트(100)가 요청한 작업이나 정보의 수행 결과를 돌려준다.

[41] 다음은, 도 2를 참고하여 본 발명의 제1 실시 예에 따른 클라이언트가 서버로 공격 패킷을 전송하여 서버에 대한 서비스 거부 공격을 수행하는 방법에 대해 설명한다.

[42] 도 2는 본 발명의 제1 실시 예에 따른 공격 패킷 전송 방법을 도시한 도면이다.

[43] 도 2에 도시된 바와 같이, 먼저, 클라이언트(100)는 서버(200)에 대한 서비스 거부 공격을 수행하기 위한 공격 패킷에 해당하는 인터넷 제어 메시지 프로토콜(Internet Control Message Protocol, 이하에서는 'ICMP'이라고도 함) 패킷을 생성한다(S110). 여기서, ICMP 패킷은 인터넷 프로토콜(Internet Protocol, 이하에서는 'IP'라고도 함) 헤더, ICMP 헤더 및 페이로드를 포함한다. 이때, 페이로드는 동일한 문자들로 구성될 수 있고, 임의의 문자들로 구성될 수도 있다.

[44] 다음, 클라이언트(100)는 생성된 ICMP 패킷의 길이에 따라 ICMP 패킷의 단편화(fragmentation) 여부를 판단한다(S120).

[45] 만약, ICMP 패킷을 단편화하는 경우, 클라이언트(100)는 ICMP 패킷의 페이로드를 분할하여 ICMP 패킷으로부터 단편화된 ICMP 패킷 즉, 복수 개의 ICMP 패킷 조각들을 생성한다(S130). 여기서, 복수 개의 ICMP 패킷 조각들 각각은 IP 헤더 및 페이로드를 포함하며, 복수 개의 ICMP 패킷 조각들 중 첫 번째 ICMP 패킷 조각은 ICMP 헤더를 더 포함한다.

[46] 이후, 클라이언트(100)는 생성된 복수 개의 ICMP 패킷 조각을 서버(200)로 전송한다(S140).

[47] 한편, ICMP 패킷을 단편화하지 아니하는 경우, 클라이언트(100)는 ICMP 패킷을 서버(200)로 전송한다(S150).

[48] 다음은, 도 3 내지 도 5를 참고하여 본 발명의 실시 예에 따른 ICMP 패킷에 대해 설명한다.

[49] 도 3은 본 발명의 실시 예에 따른 ICMP 패킷의 구조를 도시한 도면이다.

[50] 도 3에 도시된 바와 같이, ICMP 패킷(P100)은 IP 헤더(P110), ICMP 헤더(P130) 및 페이로드(P150)를 포함한다.

[51] IP 헤더(P110)는 인터넷 프로토콜(IP)과 관련된 제어정보를 포함한다.

[52] ICMP 헤더(P130)는 인터넷 제어 메시지 프로토콜(ICMP)과 관련된 제어정보를 포함한다.

[53] 페이로드(P150)는 데이터를 포함한다.

[54] 도 4는 본 발명의 실시 예에 따른 ICMP 패킷에 포함된 IP 헤더의 구조를 도시한 도면이다.

[55] 도 4에 도시된 바와 같이, IP 헤더(P110)는 IP 버전 필드(Version)(P110a), 헤더 길이 필드(Header Length)(P110b), 서비스 타입 필드(Type of Service)(P110c), 패킷 길이 필드(Total Length)(P110d), IP 식별 필드(IP Identification)(P110e), 플래그 필드(Flags)(P110f), 단편 오프셋 필드(Fragment Offset)(P110g), 패킷 유지 시간 필드(Time To Live)(P110h), 프로토콜 식별 필드(Protocol)(P110i), 헤더 체크섬(Header Checksum)(P110j), 출발지 주소 필드(Source Address)(P110k), 목적지 주소 필드(Destination Address)(P110m) 및 옵션 필드(Options)(P110n)를 포함한다.

[56] IP 버전 필드(Version)(P110a)는 해당 패킷의 IP 버전 정보를 나타내는 필드 값(field value)을 포함한다.

[57] 헤더 길이 필드(Header Length)(P110b)는 IP 헤더(P110)의 길이 정보를 나타내는 필드 값을 포함한다.

[58] 서비스 타입 필드(Type of Service)(P110c)는 서비스 품질 정보를 나타내는 필드 값을 포함한다.

[59] 패킷 길이 필드(Total Length)(P110d)는 해당 패킷의 길이 정보를 나타내는 필드 값을 포함한다.

[60] IP 식별 필드(IP Identification)(P110e)는 해당 패킷의 IP 식별 정보를 나타내는 필드 값을 포함한다.

[61] 플래그 필드(Flags)(P110f)는 해당 패킷의 단편화 특성을 나타내는 필드 값을 포함한다. 여기서, 플래그 필드(Flags)(P110f)는 해당 패킷이 마지막 패킷임을 나타내는 필드 값 즉, "0x2"를 포함할 수 있다.

[62] 단편 오프셋 필드(Fragment Offset)(P110g)는 해당 패킷의 단편화 위치를 나타내는 필드 값을 포함한다. 여기서, 단편 오프셋 필드(Fragment Offset)(P110g)는 해당 패킷이 첫 번째 패킷임을 나타내는 필드 값 즉, "0"을 포함할 수 있다.

[63] 패킷 유지 시간 필드(Time To Live)(P110h)는 해당 패킷의 폐기 여부를 결정하기 위한 패킷 유지 시간을 나타내는 필드 값을 포함한다.

[64] 프로토콜 식별 필드(Protocol)(P110i)는 해당 패킷의 프로토콜 정보를 나타내는 필드 값을 포함한다. 여기서, 프로토콜 식별 필드(Protocol)(P110i)는 인터넷 제어 메시지 프로토콜(ICMP)을 나타내는 필드 값 즉, "0x01"을 포함할 수 있다.

[65] 헤더 체크섬 필드(Header Checksum)(P110j)는 IP 헤더(P110)에 대한 오류를 검출하기 위한 체크섬을 나타내는 필드 값을 포함한다.

[66] 출발지 주소 필드(Source Address)(P110k)는 해당 패킷의 출발지의 IP 주소를 나타내는 필드 값을 포함한다.

[67] 목적지 주소 필드(Destination Address)(P110m)는 해당 패킷의 목적지 IP 주소를 나타내는 필드 값을 포함한다.

[68] 옵션 필드(Options)(P110n)는 IP 헤더(P110)의 선택 옵션을 나타내는 필드 값을 포함한다.

[69] 도 5는 본 발명의 실시 예에 따른 ICMP 패킷에 포함된 ICMP 헤더의 구조를 도시한 도면이다.

[70] 도 5에 도시된 바와 같이, ICMP 헤더(P130)는 타입 필드(Type)(P130a), 코드 필드(Code)(P130b), 체크섬 필드(Checksum)(P130c) 및 메시지 세부정보 필드(Message Specific Information)(P130d)를 포함한다.

[71] 타입 필드(Type)(P130a)는 해당 패킷의 메시지 유형을 나타내는 필드 값을 포함한다.

[72] 코드 필드(Code)(P130b)는 해당 패킷의 메시지 유형에 대한 세부정보를 나타내는 필드 값을 포함한다.

[73] 체크섬 필드(Checksum)(P130c)는 ICMP 헤더(P130)에 대한 오류를 검출하기 위한 체크섬을 나타내는 필드 값을 포함한다.

[74] 메시지 세부정보 필드(Message Specific Information)(P130d)는 해당 패킷에 대한 세부정보를 나타내는 필드 값을 포함한다.

[75] 다음은, 도 6 내지 도 8을 참고하여 본 발명의 실시 예에 따른 단편화된 ICMP 패킷에 대해 설명한다.

[76] 도 6은 본 발명의 실시 예에 따른 단편화된 ICMP 패킷의 구조를 도시한 도면이다.

[77] 도 6에 도시된 바와 같이, 단편화된 ICMP 패킷(P200)은 복수 개의 ICMP 패킷 조각들을 포함한다. 여기서, 단편화된 ICMP 패킷(P200)은 제1 ICMP 패킷 조각(P210), 제2 ICMP 패킷 조각(P220) 및 제3 ICMP 패킷 조각(P230)을 포함한다.

[78] 제1 ICMP 패킷 조각(P210)은 단편화된 ICMP 패킷(P200)의 첫 번째 패킷 조각으로써, IP 헤더(P211), ICMP 헤더(P213) 및 페이로드(P215)를 포함한다.

[79] 제2 ICMP 패킷 조각(P220)은 단편화된 ICMP 패킷(P200)의 두 번째 패킷 조각으로써, IP 헤더(P221) 및 페이로드(P225)를 포함한다.

[80] 제3 ICMP 패킷 조각(P230)은 단편화된 ICMP 패킷(P200)의 마지막 패킷 조각으로써, IP 헤더(P231) 및 페이로드(P235)를 포함한다.

[81] 도 7은 본 발명의 실시 예에 따른 ICMP 패킷 조각에 포함된 IP 헤더의 구조를 도시한 도면이다.

[82] 이때, 단편화된 ICMP 패킷(P200)에 포함된 복수 개의 ICMP 패킷 조각들 각각에 포함된 IP 헤더는 동일한 구조를 가지므로, 도 7에서는 복수 개의 ICMP 패킷 조각들 중 제1 ICMP 패킷 조각(P210)의 IP 헤더(P211)에 대해서만 설명한다.

[83] 도 7에 도시된 바와 같이, 제1 ICMP 패킷 조각(P210)의 IP 헤더(P211)는 IP 버전 필드(Version)(P211a), 헤더 길이 필드(Header Length)(P211b), 서비스 타입 필드(Type of Service)(P211c), 패킷 길이 필드(Total Length)(P211d), IP 식별 필드(IP Identification)(P211e), 플래그 필드(Flags)(P211f), 단편 오프셋 필드(Fragment Offset)(P211g), 패킷 유지 시간 필드(Time To Live)(P211h),

프로토콜 식별 필드(Protocol)(P211i), 헤더 체크섬(Header Checksum)(P211j), 출발지 주소 필드(Source Address)(P211k), 목적지 주소 필드(Destination Address)(P211m) 및 옵션 필드(Options)(P211n)를 포함한다.

[84] IP 버전 필드(Version)(P211a)는 해당 패킷의 IP 버전 정보를 나타내는 필드 값(field value)을 포함한다.

[85] 헤더 길이 필드(Header Length)(P211b)는 IP 헤더(P211)의 길이 정보를 나타내는 필드 값을 포함한다.

[86] 서비스 타입 필드(Type of Service)(P211c)는 서비스 품질 정보를 나타내는 필드 값을 포함한다.

[87] 패킷 길이 필드(Total Length)(P211d)는 해당 패킷의 길이 정보를 나타내는 필드 값을 포함한다.

[88] IP 식별 필드(IP Identification)(P211e)는 해당 패킷의 IP 식별 정보를 나타내는 필드 값을 포함한다.

[89] 플래그 필드(Flags)(P211f)는 해당 패킷의 단편화 특성 정보를 나타내는 필드 값을 포함한다. 여기서, IP 헤더(P211) 및 IP 헤더(P221)에 포함된 플래그 필드(Flags)(P211f)는 해당 패킷 조각이 마지막 패킷 조각이 아님을 나타내는 필드 값 즉, "0x1"를 포함할 수 있다. 또한, IP 헤더(P231)에 포함된 플래그 필드(Flags)(P211f)는 해당 패킷 조각이 마지막 패킷임을 나타내는 필드 값 즉, "0x2"를 포함할 수 있다.

[90] 단편 오프셋 필드(Fragment Offset)(P211g)는 해당 패킷의 단편화 위치 정보 나타내는 필드 값을 포함한다. 여기서, 단편 오프셋 필드(Fragment Offset)(P211g)는 해당 패킷 조각이 첫 번째 패킷 조각임을 나타내는 필드 값 즉, "0"을 포함할 수 있다.

[91] 패킷 유지 시간 필드(Time To Live)(P211h)는 해당 패킷의 폐기 여부를 결정하기 위한 패킷 유지 시간을 나타내는 필드 값을 포함한다.

[92] 프로토콜 식별 필드(Protocol)(P211i)는 해당 패킷의 프로토콜 정보를 나타내는 필드 값을 포함한다. 여기서, 프로토콜 식별 필드(Protocol)(P211i)는 인터넷 제어 메시지 프로토콜(ICMP)을 나타내는 필드 값 즉, "0x01"을 포함할 수 있다.

[93] 헤더 체크섬 필드(Header Checksum)(P211j)는 IP 헤더(P211)에 대한 오류를 검출하기 위한 체크섬을 나타내는 필드 값을 포함한다.

[94] 출발지 주소 필드(Source Address)(P211k)는 해당 패킷의 출발지의 IP 주소를 나타내는 필드 값을 포함한다.

[95] 목적지 주소 필드(Destination Address)(P211m)는 해당 패킷의 목적지 IP 주소를 나타내는 필드 값을 포함한다.

[96] 옵션 필드(Options)(P211n)는 IP 헤더(P211)의 선택 옵션을 나타내는 필드 값을 포함한다.

[97] 도 8은 본 발명의 실시 예에 따른 ICMP 패킷 조각에 포함된 ICMP 헤더의 구조를 도시한 도면이다.

[98] 도 8에 도시된 바와 같이, 제1 ICMP 패킷 조각(P210)의 ICMP 헤더(P213)는 타입 필드(Type)(P213a), 코드 필드(Code)(P213b), 체크섬 필드(Checksum)(P213c) 및 메시지 세부정보 필드(Message Specific Information)(P213d)를 포함한다.

[99] 타입 필드(Type)(P213a)는 해당 패킷 조각의 메시지 유형을 나타내는 필드 값을 포함한다.

[100] 코드 필드(Code)(P213b)는 해당 패킷 조각의 메시지 유형에 대한 세부정보를 나타내는 필드 값을 포함한다.

[101] 체크섬 필드(Checksum)(P213c)는 ICMP 헤더(P213)에 대한 오류를 검출하기 위한 체크섬을 나타내는 필드 값을 포함한다.

[102] 메시지 세부정보 필드(Message Specific Information)(P213d)는 해당 패킷 조각에 대한 세부정보를 나타내는 필드 값을 포함한다.

[103] 다음은, 도 9 내지 도 11을 참고하여 본 발명의 제1 실시 예에 따른 서버가 공격 패킷을 탐지 및 차단하여 서비스 거부 공격을 차단하는 방법에 대해 설명한다.

[104] 도 9는 본 발명의 제1 실시 예에 따른 서버가 서비스 거부 공격을 차단하는 방법을 도시한 도면이다.

[105] 도 9에 도시된 바와 같이, 먼저, 서버(200)는 수신된 복수 개의 패킷들 각각의 헤더 정보 및 페이로드를 이용하여 수신된 복수 개의 패킷들 중 공격 패킷을 탐지한다(S210). 여기서, 수신된 복수 개의 패킷들은 복수 개의 ICMP 패킷을 포함한다.

[106] 다음, 서버(200)는 탐지된 공격 패킷을 차단한다(S220).

[107] 도 10은 본 발명의 제1 실시 예의 하나의 예에 따른 서버가 공격 패킷을 탐지하는 방법을 도시한 도면이다.

[108] 도 10에 도시된 바와 같이, 먼저, 서버(200)는 수신된 복수 개의 패킷들 각각의 헤더 정보 즉, 프로토콜 정보, 단편화 특성 정보 및 단편화 위치 정보를 이용하여 수신된 복수 개의 패킷들 중 공격 패킷으로 의심되는 의심 패킷을 탐지한다(S311). 여기서, 서버(200)는 IP 헤더에 포함된 프로토콜 식별 필드, 플래그 필드 및 단편 오프셋 필드 각각의 필드 값을 이용하여 헤더 정보를 추출할 수 있다. 이때, 서버(200)는 프로토콜 식별 필드의 필드 값이 "0x01"이고, 플래그 필드의 필드 값이 "0x2"이며, 단편 오프셋 필드의 필드 값이 "0"인 패킷을 의심 패킷으로 결정할 수 있다.

[109] 다음, 서버(200)는 탐지된 의심 패킷에 포함된 페이로드를 이용하여 의심 패킷에 대한 공격 패킷 여부를 판단한다(S312).

[110] 만약, 의심 패킷에 포함된 페이로드가 동일한 문자들로 구성된 경우, 서버(200)는 의심 패킷을 공격 패킷으로 결정한다(S313).

[111] 이와 같이, 도 10에 따르면, 단편화되지 않은 ICMP 패킷의 페이로드가 동일한 문자들로 구성되는 공격 트래픽을 탐지할 수 있다.

[112] 도 11은 본 발명의 제1 실시 예의 다른 예에 따른 서버가 공격 패킷을 탐지하는 방법을 도시한 도면이다.

[113] 도 11에 도시된 바와 같이, 먼저, 서버(200)는 수신된 복수 개의 패킷들 각각의 헤더 정보 즉, 프로토콜 정보, 단편화 특성 정보 및 단편화 위치 정보를 이용하여 수신된 복수 개의 패킷들 중 공격 패킷으로 의심되는 의심 패킷을 탐지한다(S331). 여기서, 서버(200)는 IP 헤더에 포함된 프로토콜 식별 필드, 플래그 필드 및 단편 오프셋 필드 각각의 필드 값을 이용하여 헤더 정보를 추출할 수 있다. 이때, 서버(200)는 프로토콜 식별 필드의 필드 값이 "0x01"이고, 플래그 필드의 필드 값이 "0x2"이며, 단편 오프셋 필드의 필드 값이 "0"인 패킷을 의심 패킷으로 결정할 수 있다.

[114] 다음, 서버(200)는 탐지된 의심 패킷에 포함된 페이로드를 이용하여 의심 패킷에 대한 페이로드 정보(이하에서는 '제1 페이로드 정보'라고도 함)를 추출한다(S332). 여기서, 제1 페이로드 정보는 의심 패킷에 포함된 페이로드에 대한 페이로드의 길이 정보 및 페이로드의 해시 값을 포함한다. 이때, 서버(200)는 페이로드를 해시 함수에 적용하여 페이로드의 해시 값을 생성할 수 있다.

[115] 이후, 서버(200)는 추출된 제1 페이로드 정보를 페이로드 매칭 테이블에 저장하여 페이로드 매칭 테이블을 구성한다(S333).

[116] 다음, 서버(200)는 이후에 수신된 임의의 패킷에 대한 페이로드 정보(이하에서는 '제2 페이로드 정보'라고도 함)를 추출한다(S334).

[117] 이후, 서버(200)는 페이로드 매칭 테이블에 저장된 제1 페이로드 정보와 제2 페이로드 정보를 비교하여 임의의 패킷에 대한 공격 패킷 여부를 판단한다(S335).

[118] 만약, 제1 페이로드 정보와 제2 페이로드 정보가 동일한 경우, 서버(200)는 임의의 패킷을 공격 패킷으로 결정한다(S336).

[119] 이와 같이, 도 11에 따르면, 동일한 페이로드 문자열을 갖는 ICMP 패킷이 반복되는 공격 트래픽을 탐지할 수 있다.

[120] 다음은, 도 12 내지 도 14를 참고하여 본 발명의 제2 실시 예에 따른 서버가 공격 패킷을 탐지 및 차단하여 서비스 거부 공격을 차단하는 방법에 대해 설명한다.

[121] 도 12는 본 발명의 제2 실시 예에 따른 서버가 서비스 거부 공격을 차단하는 방법을 도시한 도면이다.

[122] 도 12에 도시된 바와 같이, 먼저, 서버(200)는 수신된 복수 개의 패킷들 각각에 대한 헤더 정보 및 페이로드를 이용하여 수신된 복수 개의 패킷들 중 공격 패킷을 탐지한다(S410). 여기서, 수신된 복수 개의 패킷들은 복수 개의 ICMP 패킷 조각을 포함한다.

[123] 다음, 서버(200)는 탐지된 공격 패킷을 차단한다(S420).

[124] 이후, 서버(200)는 차단된 공격 패킷의 IP 식별 정보를 필터링 테이블에 저장하여 필터링 테이블을 구성한다(S430). 여기서, 서버(200)는 공격 패킷의 IP 헤더에 포함된 IP 식별 필드의 필드 값을 이용하여 IP 식별 정보를 추출할 수 있다.

[125] 다음, 서버(200)는 필터링 테이블을 이용하여 패킷 필터링을 수행한다(S440). 여기서, 서버(200)는 필터링 테이블에 저장된 IP 식별 정보와 동일한 IP 식별 정보를 포함하는 패킷을 차단할 수 있다.

[126] 도 13은 본 발명의 제2 실시 예의 하나의 예에 따른 서버가 공격 패킷을 탐지하는 방법을 도시한 도면이다.

[127] 도 13에 도시된 바와 같이, 먼저, 서버(200)는 수신된 복수 개의 패킷들 각각의 헤더 정보 즉, 프로토콜 정보 및 단편화 특성 정보를 이용하여 수신된 복수 개의 패킷들 중 의심 패킷을 탐지한다(S511). 여기서, 서버(200)는 IP 헤더에 포함된 프로토콜 식별 필드 및 플래그 필드 각각의 필드 값을 이용하여 헤더 정보를 추출할 수 있다. 이때, 서버(200)는 프로토콜 식별 필드의 필드 값이 "0x01"이고, 플래그 필드의 필드 값이 "0x1"인 패킷을 의심 패킷으로 결정할 수 있다.

[128] 다음, 서버(200)는 탐지된 의심 패킷에 포함된 페이로드를 이용하여 의심 패킷에 대한 공격 패킷 여부를 판단한다(S512).

[129] 만약, 의심 패킷에 포함된 페이로드가 동일한 문자들로 구성된 경우, 서버(200)는 의심 패킷을 공격 패킷으로 결정한다(S513).

[130] 이와 같이, 도 13에 따르면, 단편화된 ICMP 패킷 조각들의 페이로드가 동일한 문자들로 구성되는 공격 트래픽을 탐지할 수 있다.

[131] 도 14는 본 발명의 제2 실시 예의 다른 예에 따른 서버가 공격 패킷을 탐지하는 방법을 도시한 도면이다.

[132] 도 14에 도시된 바와 같이, 먼저, 서버(200)는 수신된 복수 개의 패킷들 각각의 헤더 정보 즉, 프로토콜 정보, 단편화 특성 정보 및 단편화 위치 정보를 이용하여 수신된 복수 개의 패킷들 중 공격 패킷으로 의심되는 의심 패킷을 탐지한다(S531). 여기서, 서버(200)는 IP 헤더에 포함된 프로토콜 식별 필드, 플래그 필드 및 단편 오프셋 필드 각각의 필드 값을 이용하여 헤더 정보를 추출할 수 있다. 이때, 서버(200)는 프로토콜 식별 필드의 필드 값이 "0x01"이고, 플래그 필드의 필드 값이 "0x1"이며, 단편 오프셋 필드의 필드 값이 "0"인 패킷을 의심 패킷으로 결정할 수 있다.

[133] 다음, 서버(200)는 탐지된 의심 패킷에 포함된 페이로드를 이용하여 의심 패킷에 대한 페이로드 정보(이하에서는 '제1 페이로드 정보'라고도 함)를 추출한다(S532). 여기서, 제1 페이로드 정보는 의심 패킷에 포함된 페이로드에 대한 페이로드의 길이 정보 및 페이로드의 해시 값을 포함한다. 이때, 서버(200)는 페이로드를 해시 함수에 적용하여 페이로드의 해시 값을 생성할 수 있다.

[134] 이후, 서버(200)는 추출된 제1 페이로드 정보를 페이로드 매칭 테이블에 저장하여 페이로드 매칭 테이블을 구성한다(S533).

[135] 다음, 서버(200)는 이후에 수신된 임의의 패킷에 대한 페이로드 정보(이하에서는 '제2 페이로드 정보'라고도 함)를 추출한다(S534).

[136] 이후, 서버(200)는 페이로드 매칭 테이블에 저장된 제1 페이로드 정보와 제2

페이로드 정보를 비교하여 임의의 패킷에 대한 공격 패킷 여부를 판단한다(S535).

[137] 만약, 제1 페이로드 정보와 제2 페이로드 정보가 동일한 경우, 서버(200)는 임의의 패킷을 공격 패킷으로 결정한다(S536).

[138] 이와 같이, 도 14에 따르면, 동일한 페이로드 문자열을 갖는 ICMP 패킷이 단편화되어 반복되는 공격 트래픽을 탐지할 수 있다.

[139] 다음은, 도 15를 참고하여 본 발명의 제3 실시 예에 따른 서버가 공격 패킷을 탐지 및 차단하여 서비스 거부 공격을 차단하는 방법에 대해 설명한다.

[140] 도 15는 본 발명의 제3 실시 예에 따른 서버가 서비스 거부 공격을 차단하는 방법을 도시한 도면이다.

[141] 도 15에 도시된 바와 같이, 먼저, 서버(200)는 수신된 복수 개의 패킷들 각각의 헤더 정보 즉, 프로토콜 정보 및 단편화 특성 정보를 이용하여 수신된 복수 개의 패킷들 중 의심 패킷을 탐지한다(S610). 여기서, 서버(200)는 IP 헤더에 포함된 프로토콜 식별 필드 및 플래그 필드 각각의 필드 값을 이용하여 헤더 정보를 추출할 수 있다. 이때, 서버(200)는 프로토콜 식별 필드의 필드 값이 "0x01"이고, 플래그 필드의 필드 값이 "0x1"인 패킷을 의심 패킷으로 결정할 수 있다.

[142] 다음, 서버(200)는 일정 시간 동안에 수신되는 의심 패킷의 수신량을 측정한다(S620). 이때, 서버(200)는 의심 패킷의 수신 빈도를 측정할 수 있다.

[143] 이후, 서버(200)는 의심 패킷의 수신량과 미리 정해진 임계치를 비교하여 의심 패킷의 수신량이 임계치를 초과하는지를 판단한다(S630).

[144] 만약, 의심 패킷의 수신량이 임계치를 초과하는 경우, 서버(200)는 이후에 수신되는 의심 패킷을 차단한다(S640).

[145] 이와 같이, 도 15에 따르면, ICMP 패킷의 페이로드에 특정 규칙이 존재하지 않으면서 단편화된 공격 트래픽을 탐지 및 차단할 수 있다.

[146] 다음은, 도 16을 참고하여 본 발명의 제2 실시 예에 따른 클라이언트가 서버로 공격 패킷을 전송하여 서버에 대한 서비스 거부 공격을 수행하는 방법에 대해 설명한다.

[147] 도 16은 본 발명의 제2 실시 예에 따른 공격 패킷 전송 방법을 도시한 도면이다.

[148] 도 16에 도시된 바와 같이, 먼저, 클라이언트(100)는 서버(200)에 대한 서비스 거부 공격을 수행하기 위한 공격 패킷에 해당하는 ICMP 질의 메시지를 생성한다(S710). 여기서, ICMP 질의 메시지는 IP 헤더, ICMP 헤더 및 페이로드를 포함한다.

[149] 다음, 클라이언트(100)는 생성된 ICMP 질의 메시지를 서버(200)로 전송한다(S720).

[150] 다음은, 도 17 내지 도 19를 참고하여 본 발명의 실시 예에 따른 ICMP 질의 메시지에 대해 설명한다.

[151] 도 17은 본 발명의 실시 예에 따른 ICMP 질의 메시지의 구조를 도시한 도면이다.

[152] 도 17에 도시된 바와 같이, ICMP 질의 메시지(P300)는 IP 헤더(P310), ICMP 헤더(P330) 및 페이로드(P350)를 포함한다.

[153] IP 헤더(P310)는 인터넷 프로토콜(IP)과 관련된 제어정보를 포함한다.

[154] ICMP 헤더(P330)는 인터넷 제어 메시지 프로토콜(ICMP)과 관련된 제어정보를 포함한다.

[155] 페이로드(P350)는 데이터를 포함한다.

[156] 도 18은 본 발명의 실시 예에 따른 ICMP 질의 메시지에 포함된 IP 헤더의 구조를 도시한 도면이다.

[157] 도 18에 도시된 바와 같이, IP 헤더(P310)는 IP 버전 필드(Version)(P310a), 헤더 길이 필드(Header Length)(P310b), 서비스 타입 필드(Type of Service)(P310c), 패킷 길이 필드(Total Length)(P310d), IP 식별 필드(IP Identification)(P310e), 플래그 필드(Flags)(P310f), 단편 오프셋 필드(Fragment Offset)(P310g), 패킷 유지 시간 필드(Time To Live)(P310h), 프로토콜 식별 필드(Protocol)(P310i), 헤더 체크섬(Header Checksum)(P310j), 출발지 주소 필드(Source Address)(P310k), 목적지 주소 필드(Destination Address)(P310m) 및 옵션 필드(Options)(P310n)를 포함한다.

[158] IP 버전 필드(Version)(P310a)는 해당 패킷의 IP 버전 정보를 나타내는 필드 값(field value)을 포함한다.

[159] 헤더 길이 필드(Header Length)(P310b)는 IP 헤더(P310)의 길이 정보를 나타내는 필드 값을 포함한다.

[160] 서비스 타입 필드(Type of Service)(P310c)는 서비스 품질 정보를 나타내는 필드 값을 포함한다.

[161] 패킷 길이 필드(Total Length)(P310d)는 해당 패킷의 길이 정보를 나타내는 필드 값을 포함한다.

[162] IP 식별 필드(IP Identification)(P310e)는 해당 패킷의 IP 식별 정보를 나타내는 필드 값을 포함한다.

[163] 플래그 필드(Flags)(P310f)는 해당 패킷의 단편화 특성을 나타내는 필드 값을 포함한다.

[164] 단편 오프셋 필드(Fragment Offset)(P310g)는 해당 패킷의 단편화 위치를 나타내는 필드 값을 포함한다.

[165] 패킷 유지 시간 필드(Time To Live)(P310h)는 해당 패킷의 폐기 여부를 결정하기 위한 패킷 유지 시간을 나타내는 필드 값을 포함한다.

[166] 프로토콜 식별 필드(Protocol)(P310i)는 해당 패킷의 프로토콜 정보를 나타내는 필드 값을 포함한다. 여기서, 프로토콜 식별 필드(Protocol)(P310i)는 인터넷 제어 메시지 프로토콜(ICMP)을 나타내는 필드 값 즉, "0x01"을 포함할 수 있다.

[167] 헤더 체크섬 필드(Header Checksum)(P310j)는 IP 헤더(P310)에 대한 오류를 검출하기 위한 체크섬을 나타내는 필드 값을 포함한다.

[168] 출발지 주소 필드(Source Address)(P310k)는 해당 패킷의 출발지 IP 주소를

나타내는 필드 값을 포함한다.

[169] 목적지 주소 필드(Destination Address)(P310m)는 해당 패킷의 목적지 IP 주소를 나타내는 필드 값을 포함한다.

[170] 옵션 필드(Options)(P310n)는 IP 헤더(P310)의 선택 옵션을 나타내는 필드 값을 포함한다.

[171] 도 19는 본 발명의 실시 예에 따른 ICMP 질의 메시지에 포함된 ICMP 헤더의 구조를 도시한 도면이다.

[172] 도 19에 도시된 바와 같이, ICMP 헤더(P330)는 타입 필드(Type)(P330a), 코드 필드(Code)(P330b), 체크섬 필드(Checksum)(P330c), 식별자 필드(Identifier)(P330d) 및 시퀀스 번호 필드(Sequence Number)(P330e)를 포함한다.

[173] 타입 필드(Type)(P330a)는 메시지 유형 정보를 나타내는 필드 값을 포함한다. 이때, 타입 필드(Type)(P330a)는 해당 패킷의 메시지 유형이 반향 요청(echo request)임을 나타내는 필드 값 즉, "0x8"을 포함할 수 있다. 또한, 타입 필드(Type)(P330a)는 해당 패킷의 메시지 유형이 반향 응답(echo reply)임을 나타내는 필드 값 즉, "0x0"을 포함할 수 있다.

[174] 코드 필드(Code)(P330b)는 메시지 유형에 따른 메시지 유형 하위 정보를 나타내는 필드 값을 포함한다. 여기서, 해당 패킷의 메시지 유형이 반향 요청 또는 반향 응답인 경우, 코드 필드(Code)(P330b)는 "0x0"의 필드 값을 포함할 수 있다.

[175] 체크섬 필드(Checksum)(P330c)는 ICMP 헤더(P330)에 대한 오류를 검출하기 위한 체크섬을 나타내는 필드 값을 포함한다.

[176] 식별자 필드(Identifier)(P330d)는 ICMP 질의 메시지에 대한 메시지 식별 정보를 나타내는 필드 값을 포함한다. 이때, ICMP 질의 메시지는 메시지 유형 정보에 따라 반향 요청 메시지 및 반향 응답 메시지로 구분되며, 반향 요청 메시지와 반향 응답 메시지는 식별자 필드(Identifier)(P330d)의 필드 값이 동일하다.

[177] 시퀀스 번호 필드(Sequence Number)(P330e)는 ICMP 질의 메시지의 시퀀스 정보를 나타내는 필드 값을 포함한다.

[178] 다음은, 도 20 내지 도 23을 참고하여 본 발명의 제4 실시 예에 따른 서버가 공격 패킷을 탐지 및 차단하여 서비스 거부 공격을 차단하는 방법에 대해 설명한다.

[179] 도 20은 본 발명의 제4 실시 예에 따른 서버가 서비스 거부 공격을 차단하는 방법을 도시한 도면이다.

[180] 도 20에 도시된 바와 같이, 먼저, 서버(200)는 수신된 복수 개의 패킷들 각각의 헤더 정보를 이용하여 수신된 복수 개의 패킷들 중 공격 패킷을 탐지한다(S810). 여기서, 수신된 복수 개의 패킷들은 복수 개의 ICMP 질의 메시지를 포함한다.

[181] 다음, 서버(200)는 탐지된 공격 패킷을 차단한다(S820).

[182] 도 21은 본 발명의 제4 실시 예의 하나의 예에 따른 서버가 공격 패킷을 탐지하는 방법을 도시한 도면이다.

[183] 도 21에 도시된 바와 같이, 먼저, 서버(200)는 수신된 복수 개의 패킷들 각각의 헤더 정보 즉, 프로토콜 정보, 메시지 유형 정보 및 메시지 유형 하위 정보를 이용하여 수신된 복수 개의 패킷들 중 의심 패킷을 탐지한다(S911). 여기서, 서버(200)는 IP 헤더에 포함된 프로토콜 식별 필드, ICMP 헤더에 포함된 타입 필드 및 코드 필드 각각의 필드 값을 이용하여 헤더 정보를 추출할 수 있다. 이때, 서버(200)는 프로토콜 식별 필드의 필드 값이 "0x01"이고, 타입 필드의 필드 값이 "0x8"이며, 코드 필드의 필드 값이 "0x0"인 패킷을 의심 패킷으로 결정할 수 있다.

[184] 다음, 서버(200)는 탐지된 의심 패킷에 대한 주소 정보(이하에서는 '제1 주소 정보'라고도 함)를 추출한다(S912). 여기서, 추출된 주소 정보는 의심 패킷의 출발지 IP 주소 및 목적지 IP 주소를 포함한다.

[185] 이후, 서버(200)는 제1 주소 정보를 필터링 테이블에 저장하여 필터링 테이블을 구성한다(S913).

[186] 다음, 서버(200)는 이후에 수신된 임의의 ICMP 질의 메시지에 대한 주소 정보(이하에서는 '제2 주소 정보'라고도 함)를 추출한다(S914). 여기서, 임의의 ICMP 질의 메시지는 프로토콜 식별 필드의 필드 값이 "0x01"이고, 타입 필드의 필드 값이 "0x8"이며, 코드 필드의 필드 값이 "0x0"인 반향 요청 메시지이다.

[187] 이후, 서버(200)는 필터링 테이블에 저장된 제1 주소 정보와 제2 주소 정보를 비교하여 수신된 ICMP 질의 메시지에 대한 공격 패킷 여부를 판단한다(S915).

[188] 만약, 제2 주소 정보와 미전송된 반향 응답 메시지에 포함된 제1 주소 정보가 동일한 경우, 서버(200)는 임의의 ICMP 질의 메시지를 공격 패킷으로 결정한다(S916).

[189] 이와 같이, 도 21에 따르면, ICMP 반향 요청 플러딩 또는 핑(Ping) 플러딩 공격을 시도하는 공격 트래픽을 탐지할 수 있다.

[190] 도 22는 본 발명의 제4 실시 예의 다른 예에 따른 서버가 공격 패킷을 탐지하는 방법을 도시한 도면이다.

[191] 도 22에 도시된 바와 같이, 먼저, 서버(200)는 ICMP 질의 메시지를 수신한다(S931). 여기서, ICMP 질의 메시지는 프로토콜 식별 필드의 필드 값이 "0x01"이고, 타입 필드의 필드 값이 "0x8"이며, 코드 필드의 필드 값이 "0x0"인 반향 요청 메시지이다.

[192] 다음, 서버(200)는 수신된 ICMP 질의 메시지의 헤더 정보를 추출한다(S932). 여기서, 추출된 헤더 정보는 ICMP 질의 메시지의 목적지 IP 주소, 메시지 식별 정보 및 시퀀스 정보를 포함한다. 이때, 서버(200)는 IP 헤더에 포함된 목적지 주소 필드, ICMP 헤더에 포함된 식별자 필드 및 시퀀스 번호 필드 각각의 필드 값을 이용하여 헤더 정보를 추출할 수 있다.

[193] 이후, 서버(200)는 수신된 복수 개의 패킷들 중 추출된 헤더 정보에 대응되는 의심 패킷을 탐지한다(S933). 여기서, 탐지된 의심 패킷의 헤더 정보는 ICMP 질의 메시지의 헤더 정보와 동일하다.

[194] 다음, 서버(200)는 ICMP 질의 메시지와 의심 패킷간의 수신 시간차와 미리

정해진 기준 시간을 비교하여 의심 패킷에 대한 공격 패킷 여부를 판단한다(S934). 여기서, 수신 시간차는 ICMP 질의 메시지가 수신된 시각과 의심 패킷이 수신된 시각의 시간 차를 나타낸다.

[195] 만약, 수신 시간차가 기준 시간 이내인 경우, 서버(200)는 의심 패킷을 공격 패킷으로 결정한다(S935). 여기서, 서버(200)는 ICMP 질의 메시지도 공격 패킷으로 결정할 수 있다. 예를 들어, ICMP 질의 메시지와 의심 패킷간의 수신 시간차가 1초 이내인 경우, 의심 패킷을 공격 패킷으로 결정할 수 있다.

[196] 이와 같이, 도 22에 따르면, 반복되는 ICMP 질의 메시지의 메시지 식별 정보와 시퀀스 정보가 동일한 공격 트래픽을 탐지할 수 있다.

[197] 도 23은 본 발명의 제4 실시 예의 또 다른 예에 따른 서버가 공격 패킷을 탐지하는 방법을 도시한 도면이다.

[198] 도 23에 도시된 바와 같이, 먼저, 서버(200)는 수신된 복수 개의 패킷들 각각의 헤더 정보 즉, 프로토콜 정보, 메시지 유형 정보 및 메시지 유형 하위 정보를 이용하여 수신된 복수 개의 패킷들 중 의심 패킷을 탐지한다(S911). 여기서, 서버(200)는 IP 헤더에 포함된 프로토콜 식별 필드, ICMP 헤더에 포함된 타입 필드 및 코드 필드 각각의 필드 값을 이용하여 헤더 정보를 추출할 수 있다. 이때, 서버(200)는 프로토콜 식별 필드의 필드 값이 "0x01"이고, 타입 필드의 필드 값이 "0x0"이며, 코드 필드의 필드 값이 "0x0"인 패킷 즉, 반향 응답 메시지를 의심 패킷으로 결정할 수 있다.

[199] 다음, 서버(200)는 탐지된 의심 패킷의 주소 정보를 추출한다(S952). 여기서, 추출된 주소 정보는 의심 패킷의 출발지 IP 주소 및 목적지 IP 주소를 포함한다.

[200] 이후, 서버(200)는 추출된 주소 정보와 미리 저장된 필터링 테이블을 비교하여 의심 패킷에 대한 공격 패킷 여부를 판단한다(S953). 여기서 필터링 테이블은 전송된 반향 요청 메시지의 주소 정보를 저장한다.

[201] 만약, 추출된 주소 정보가 필터링 테이블에 저장되어 있지 아니한 경우, 서버(200)는 의심 패킷을 공격 패킷으로 결정한다(S954).

[202] 이와 같이, 도 23에 따르면, 공격 대상 서버로 반향 요청 메시지 없이 반향 응답 메시지가 폭주하는 형태의 공격 트래픽을 탐지할 수 있다.

[203] 이상에서와 같이 도면과 명세서에서 최적의 실시 예가 개시되었다. 여기서 특정한 용어들이 사용되었으나, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미 한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

청구범위

[청구항 1] 서버가 인터넷 제어 메시지 프로토콜을 이용한 공격 패킷을 차단하는 서비스 거부 공격 차단 방법에 있어서,
상기 인터넷 제어 메시지 프로토콜을 따르는 제1 반향 요청 메시지를 수신하는 단계;
상기 제1 반향 요청 메시지의 헤더 정보에서 필터링 정보를 추출하는 단계;
상기 인터넷 제어 메시지 프로토콜을 따르는 제2 반향 요청 메시지를 수신하는 단계; 및
상기 제2 반향 요청 메시지의 헤더 정보와 상기 필터링 정보를 비교하여 상기 제2 반향 요청 메시지에 대한 공격 패킷 여부를 결정하는 단계를 포함하는 서비스 거부 공격 차단 방법.

[청구항 2] 제1항에 있어서,
상기 결정하는 단계는
상기 제2 반향 요청 메시지의 헤더 정보가 상기 필터링 정보에 포함된 주소 정보에 대응되는 경우, 상기 제2 반향 요청 메시지를 공격 패킷으로 결정하는 서비스 거부 공격 차단 방법.

[청구항 3] 제2항에 있어서,
상기 필터링 정보는
상기 제1 반향 요청 메시지의 헤더 정보에 포함된 출발지 주소 정보 및 목적지 주소 정보를 포함하는 서비스 거부 공격 차단 방법.

[청구항 4] 제1항에 있어서,
상기 결정하는 단계는
상기 제2 반향 요청 메시지의 헤더 정보가 상기 필터링 정보에 대응되는 경우, 상기 제2 반향 요청 메시지를 의심 패킷으로 결정하는 단계; 및
상기 제1 반향 요청 메시지에 대한 응답 메시지를 전송하기 전에 상기 제2 반향 요청 메시지가 수신된 경우, 상기 의심 패킷을 공격 패킷으로 결정하는 서비스 거부 공격 차단 방법.

[청구항 5] 제4항에 있어서,
상기 필터링 정보는
상기 제1 반향 요청 메시지의 헤더 정보에 포함된 출발지 주소 정보 및 목적지 주소 정보를 포함하는 서비스 거부 공격 차단 방법.

[청구항 6] 제1항에 있어서,
상기 결정하는 단계는
상기 제2 반향 요청 메시지의 헤더 정보와 상기 필터링 정보 각각의 메시지 식별 정보 및 시퀀스 정보가 동일한 경우, 상기 제2

반향 요청 메시지를 공격 패킷으로 결정하는 서비스 거부 공격 차단 방법.

[청구항 7] 제1항에 있어서,
상기 결정하는 단계는
상기 제2 반향 요청 메시지의 헤더 정보가 상기 필터링 정보에 대응되는 경우, 상기 제2 반향 요청 메시지를 의심 패킷으로 결정하는 단계; 및
상기 제1 반향 요청 메시지의 수신 시각과 상기 제2 반향 요청 메시지의 수신 시각의 시간 차가 기준 시간 이내인 경우, 상기 제2 반향 요청 메시지를 공격 패킷으로 결정하는 단계를 포함하는 서비스 거부 공격 차단 방법.

[청구항 8] 제7항에 있어서,
상기 공격 패킷으로 결정하는 단계는
상기 제1 반향 요청 메시지를 공격 패킷으로 결정하는 서비스 거부 공격 차단 방법.

[청구항 9] 제7항에 있어서,
상기 필터링 정보는
상기 제1 반향 요청 메시지의 헤더 정보에 포함된 목적지 주소 정보, 메시지 식별 정보 및 시퀀스 정보를 포함하는 서비스 거부 공격 차단 방법.

[청구항 10] 서버가 인터넷 제어 메시지 프로토콜을 이용한 공격 패킷을 차단하는 서비스 거부 공격 차단 방법에 있어서,
수신된 복수 개의 패킷들 각각의 헤더 정보를 이용하여 상기 복수 개의 패킷들 중에서 의심 패킷을 추출하는 단계;
상기 의심 패킷의 헤더 정보에서 필터링 정보를 추출하는 단계;
상기 인터넷 제어 메시지 프로토콜을 따르는 메시지를 수신하는 단계; 및
상기 필터링 정보와 상기 메시지의 헤더 정보를 비교하여 상기 메시지에 대한 공격 패킷 여부를 결정하는 단계를 포함하는 서비스 거부 공격 차단 방법.

[청구항 11] 제10항에 있어서,
상기 의심 패킷을 추출하는 단계는
상기 복수 개의 패킷들 각각의 프로토콜 정보 및 메시지 유형 정보를 이용하여 상기 복수 개의 패킷들 중에서 상기 의심 패킷을 추출하는 서비스 거부 공격 차단 방법.

[청구항 12] 제11항에 있어서,
상기 필터링 정보를 추출하는 단계는
상기 의심 패킷의 헤더 정보에서 출발지 주소 정보 및 목적지 주소

정보를 포함하는 필터링 정보를 추출하는 서비스 거부 공격 차단 방법.

[청구항 13] 제12항에 있어서,
상기 결정하는 단계는
상기 메시지의 헤더 정보가 상기 필터링 정보와 대응되는 경우, 상기 의심 패킷에 대한 응답 패킷의 전송 시각과 상기 메시지의 수신 시각을 비교하는 단계; 및
상기 메시지의 수신 시각이 상기 응답 패킷의 전송 시각보다 빠른 경우, 상기 메시지를 공격 패킷으로 결정하는 단계를 포함하는 서비스 거부 공격 차단 방법.

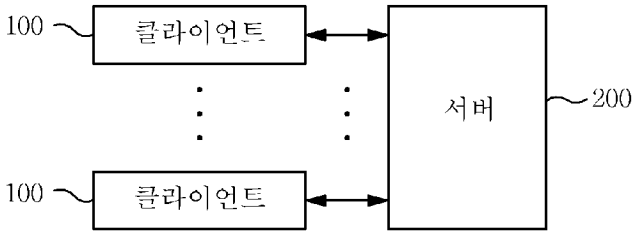
[청구항 14] 제11항에 있어서,
상기 의심 패킷을 추출하는 단계는
반향 요청 메시지를 수신하는 단계;
상기 반향 요청 메시지의 헤더 정보를 추출하는 단계; 및
상기 반향 요청 메시지의 헤더 정보와 상기 복수 개의 패킷들 각각의 헤더 정보를 비교하여 상기 의심 패킷을 추출하는 단계를 포함하는 서비스 거부 공격 차단 방법.

[청구항 15] 제14항에 있어서,
상기 필터링 정보를 추출하는 단계는
상기 의심 패킷의 헤더 정보에서 메시지 식별 정보 및 시퀀스 정보를 포함하는 필터링 정보를 추출하는 서비스 거부 공격 차단 방법.

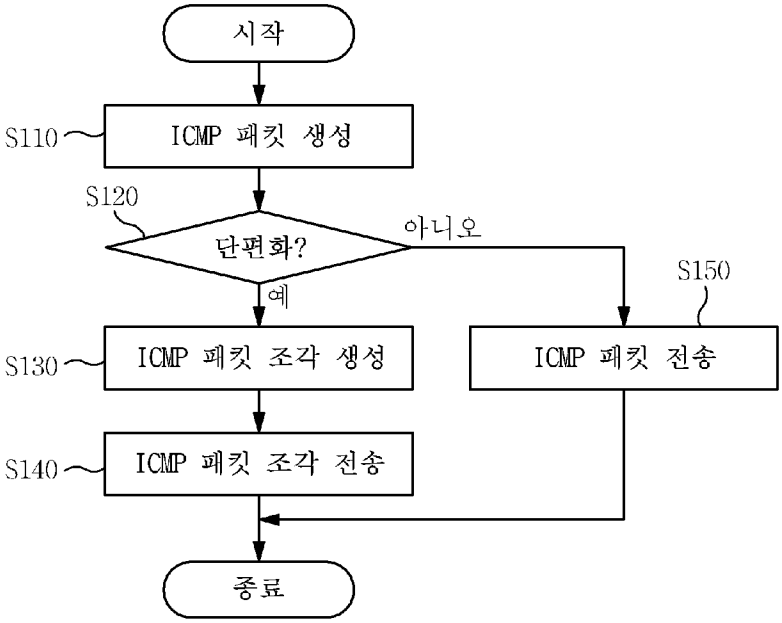
[청구항 16] 제15항에 있어서,
상기 결정하는 단계는
상기 메시지의 헤더 정보가 상기 필터링 정보와 대응되는 경우, 상기 의심 패킷의 수신 시각과 상기 메시지의 수신 시각간의 시간차를 계산하는 단계; 및
상기 시간차가 미리 정해진 기준 시간 이내인 경우, 상기 메시지를 공격 패킷으로 결정하는 단계를 포함하는 서비스 거부 공격 차단 방법.

[청구항 17] 제11항에 있어서,
상기 의심 패킷은
상기 인터넷 제어 메시지 프로토콜을 따르는 질의 메시지인 서비스 거부 공격 차단 방법.

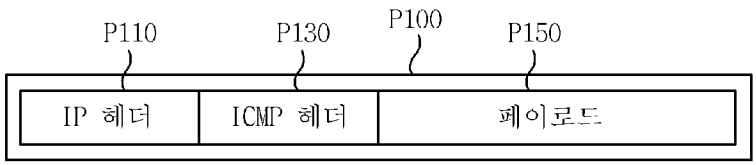
[Fig. 1]



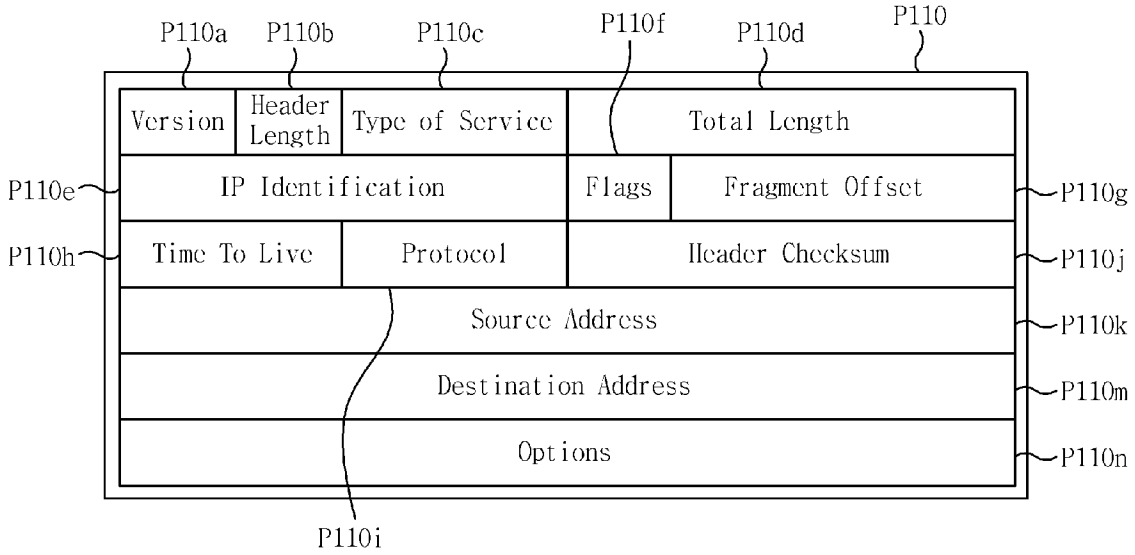
[Fig. 2]



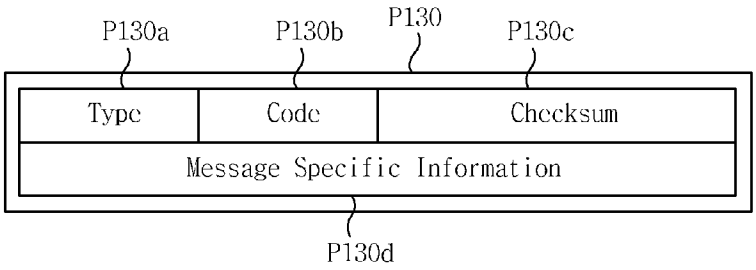
[Fig. 3]



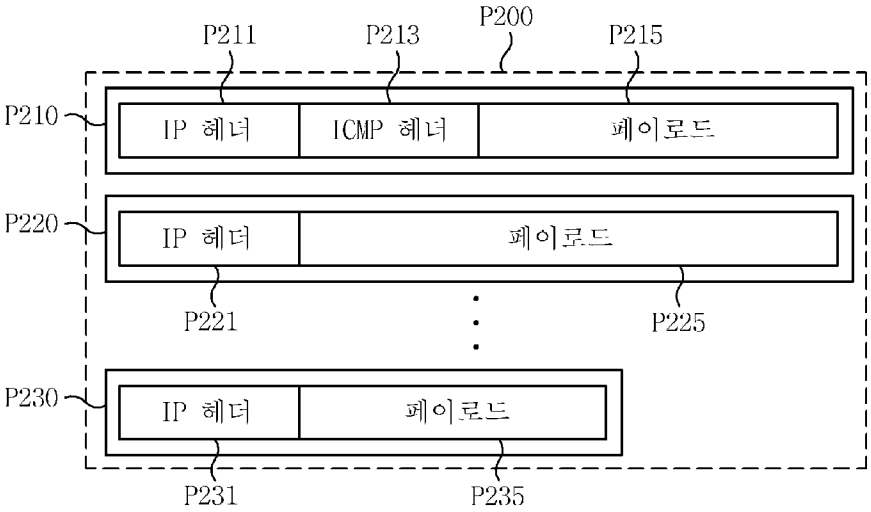
[Fig. 4]



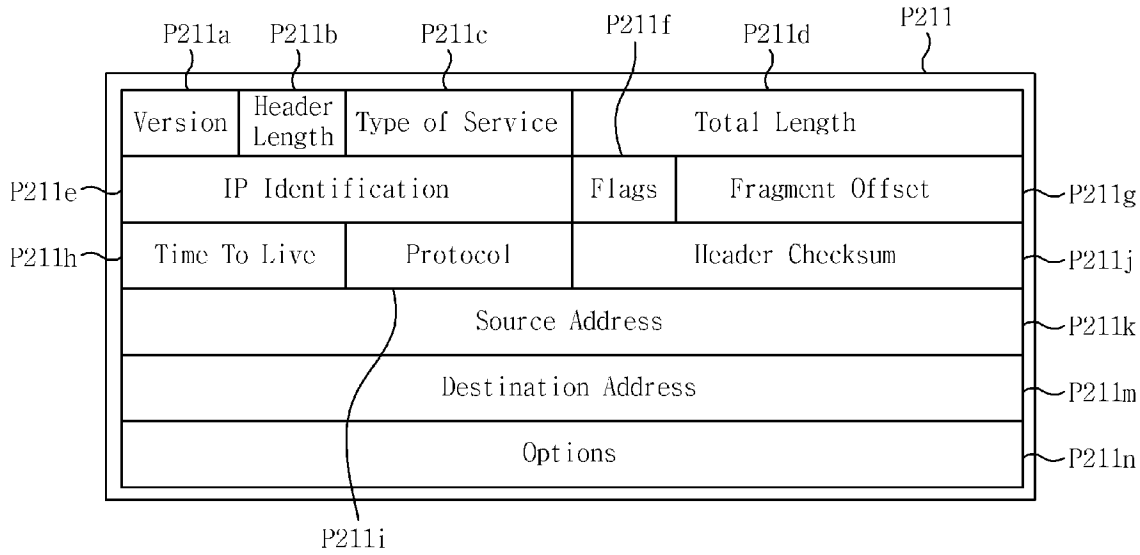
[Fig. 5]



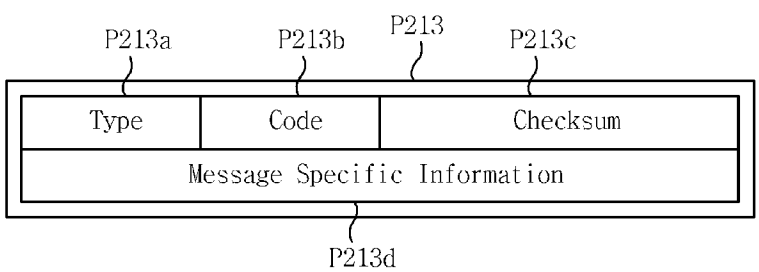
[Fig. 6]



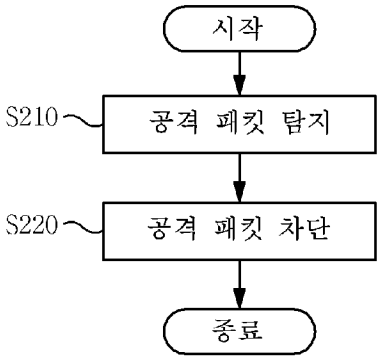
[Fig. 7]



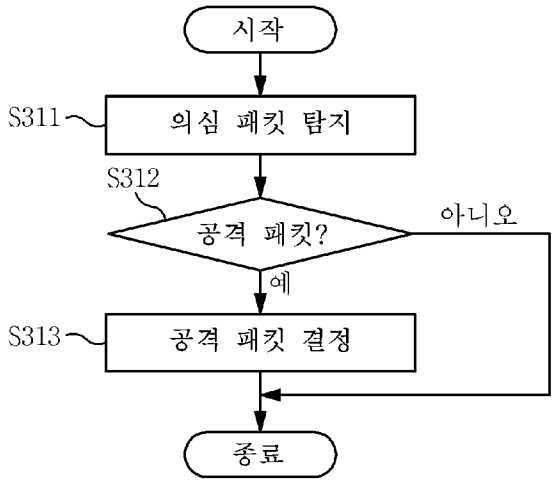
[Fig. 8]



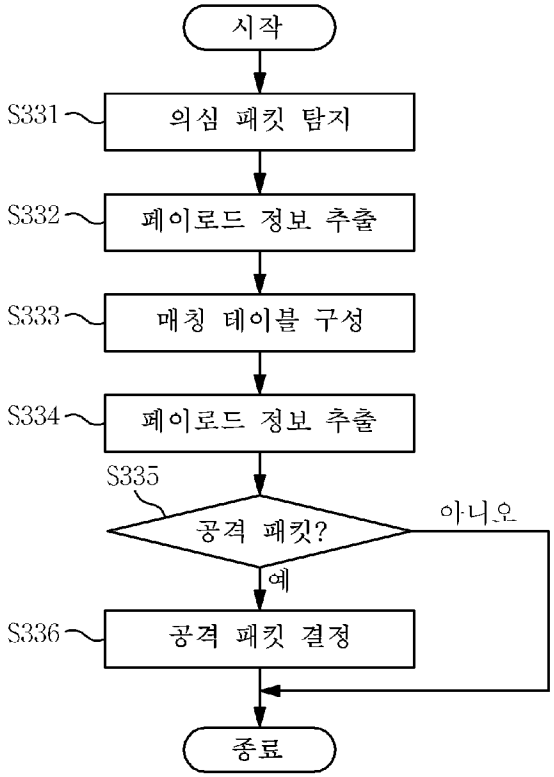
[Fig. 9]



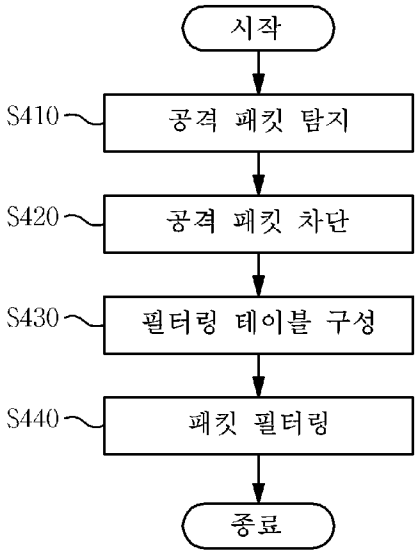
[Fig. 10]



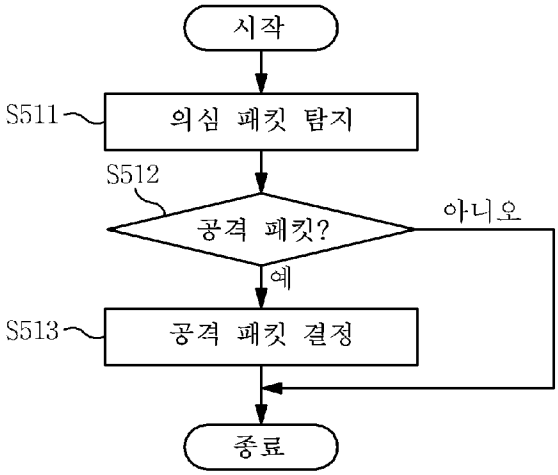
[Fig. 11]



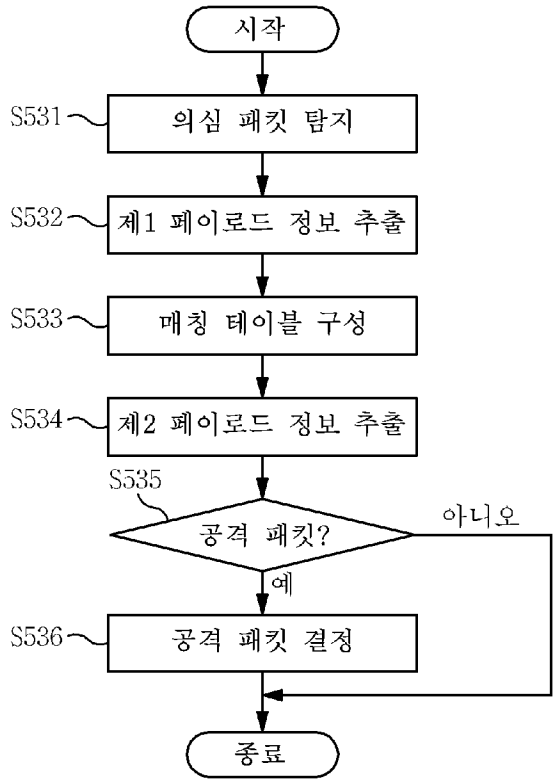
[Fig. 12]


시작
S410
공격 패킷 탐지
S420
공격 패킷 차단
S430
필터링 테이블 구성
S440
패킷 필터링
종료

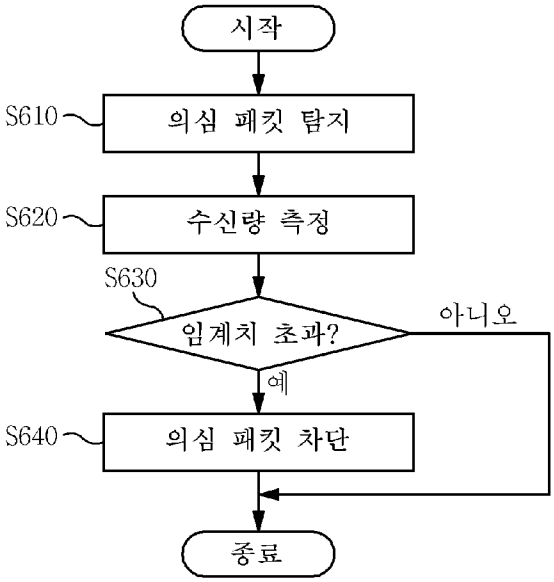
[Fig. 13]


시작
S511
의심 패킷 탐지
S512
공격 패킷?
아니오
예
S513
공격 패킷 결정
종료

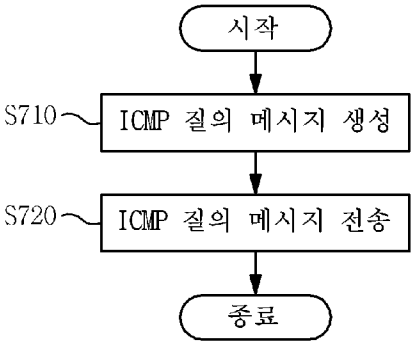
[Fig. 14]



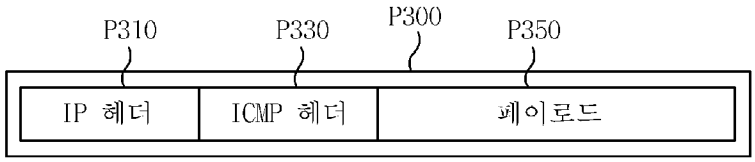
[Fig. 15]



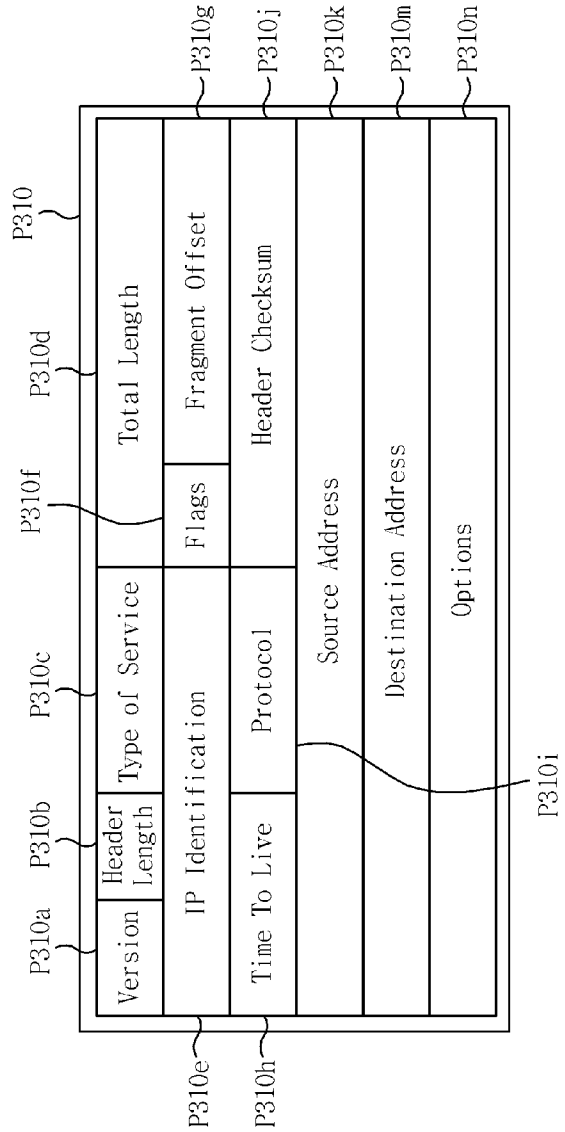
[Fig. 16]



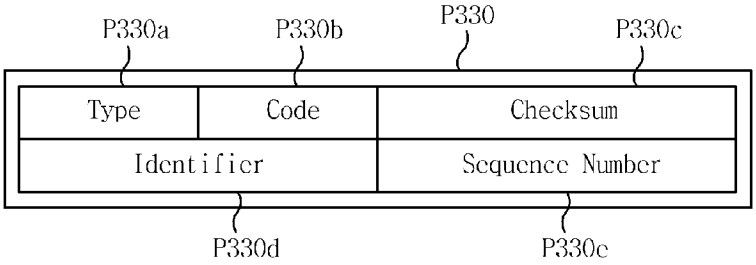
[Fig. 17]



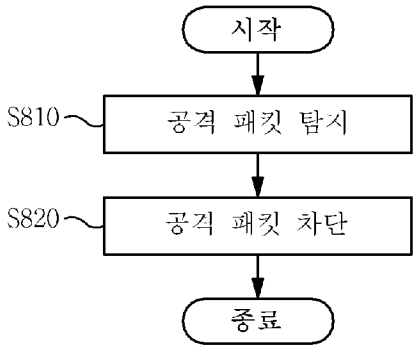
[Fig. 18]



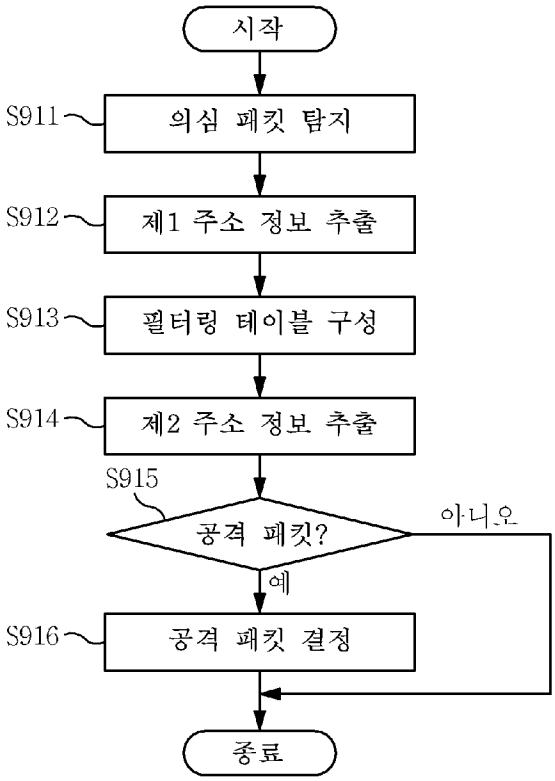
[Fig. 19]



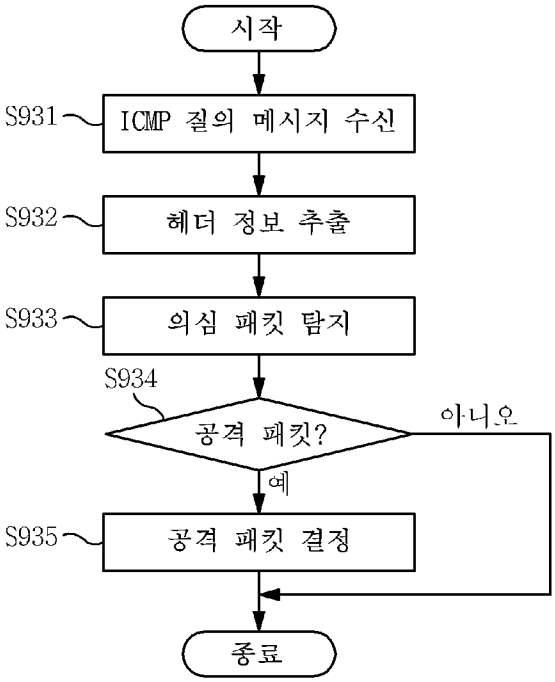
[Fig. 20]


시작
S810
공격 패킷 탐지
S820
공격 패킷 차단
종료

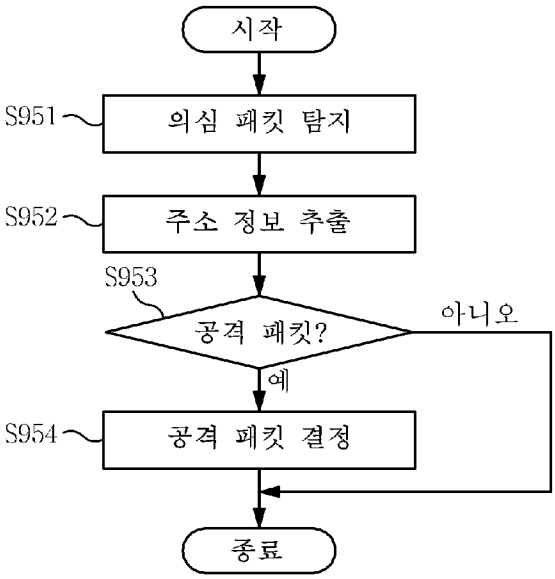
[Fig. 21]


시작
S911
의심 패킷 탐지
S912
제1 주소 정보 추출
S913
필터링 테이블 구성
S914
제2 주소 정보 추출
S915
공격 패킷?
아니오
예
S916
공격 패킷 결정
종료

[Fig. 22]


시작
S931
ICMP 질의 메시지 수신
S932
헤더 정보 추출
S933
의심 패킷 탐지
S934
공격 패킷?
아니오
예
S935
공격 패킷 결정
종료

[Fig. 23]


시작
S951
의심 패킷 탐지
S952
주소 정보 추출
S953
공격 패킷?
아니오
예
S954
공격 패킷 결정
종료

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2011/009619

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/22(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 12/22; H04L 12/26; H04L 12/50; H04L 12/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: Internet Control Message protocol (ICMP), echo request

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	KR 10-2003-0094839 A (LG ELECTRONICS INC.) 18 December 2003 See abstract, paragraphs <20>, <24>-<43>, claims 2,3 and figures 1-3.	1,10 2-9,11-17
Y A	US 2006-0098585 A1 (CISCO TECHNOLOGY, INC) 11 May 2006 See abstract, paragraphs <21>-<24>, <27>,<28>, claims 1-13 and figures 1-3.	1,10 2-,11-17
A	KR 10-2003-0049288 A (CLIPCOMM INC.) 25 June 2003 See abstract, paragraphs <12>-<18>, <31>-<33>, claims 1-8 and figure 4.	1-17

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 MARCH 2012 (27.03.2012)	**28 MARCH 2012 (28.03.2012)**

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Daejeon 302-701,
Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2011/009619

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2003-0094839 A	18.12.2003	NONE	
US 2006-0098585 A1	11.05.2006	US 2006-0098687 A1	11.05.2006
		US 7535909 B2	19.05.2009
		US 7936682 B2	03.05.2011
KR 10-2003-0049288 A	25.06.2003	NONE	

국 제 조 사 보 고 서

국제출원번호
PCT/KR2011/009619

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 12/22(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
H04L 12/22; H04L 12/26; H04L 12/50; H04L 12/56

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: 인터넷 제어 메시지 프로토콜(ICMP), 반향 요청

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y A	KR 10-2003-0094839 A (엘지전자 주식회사) 2003.12.18 요약, 단락 <20>, <24>-<43>, 청구항 2,3 및 도면 1-3 참조.	1,10 2-9,11-17
Y A	US 2006-0098585 A1 (씨스코 테크놀로지 인크.) 2006.05.11 요약, 단락 <21>-<24>, <27>, <28>, 청구항 1-13 및 도면 1-3 참조.	1,10 2-9,11-17
A	KR 10-2003-0049288 A ((주)클립컴) 2003.06.25 요약, 단락 <12>-<18>, <31>-<33>, 청구항 1-8 및 도면 4 참조.	1-17

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2012년 03월 27일 (27.03.2012)	**2012년 03월 28일 (28.03.2012)**

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
정부대전청사
팩스 번호 82-42-472-7140

심사관
홍경아
전화번호 82-42-481-5668

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2011/009619

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2003-0094839 A	2003.12.18	없음	
US 2006-0098585 A1	2006.05.11	US 2006-0098687 A1	2006.05.11
		US 7535909 B2	2009.05.19
		US 7936682 B2	2011.05.03
KR 10-2003-0049288 A	2003.06.25	없음	