

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국



(10) 국제공개번호
WO 2011/002119 A1

PCT

(43) 국제공개일
2011년 1월 6일 (06.01.2011)

- (51) 국제특허분류:
H04L 12/26 (2006.01)
- (21) 국제출원번호: PCT/KR2009/003693
- (22) 국제출원일: 2009년 7월 7일 (07.07.2009)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2009-0060201 2009년 7월 2일 (02.07.2009) KR
- (71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): **충남대학교 산학협력단 (THE INDUSTRY & ACADEMIC COOPERATION IN CHUNGNAM NATIONAL UNIVERSITY (IAC))** [KR/KR]; 대전 유성구 궁동 220 충남대학교, 305-764 Daejeon (KR).
- (72) 발명자: **김**
- (75) 발명자/출원인 (US 에 한하여): **김형식 (KIM, Hyong-Shik)** [KR/KR]; 대전 유성구 엑스포로 286 엑스포아파트 206-1306, 305-761 Daejeon (KR).
- (74) 대리인: **김원준 (KIM, Wonjoon)**; 대전시 서구 만년동 386 골드벤처타워 205 호, 302-823 Daejeon (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, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 유럽 (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, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

규칙 4.17 에 의한 선언서:

- 신규성을 해치지 아니하는 개시 또는 신규성 상실의 예외에 관한 선언 (규칙 4.17(v))

공개:

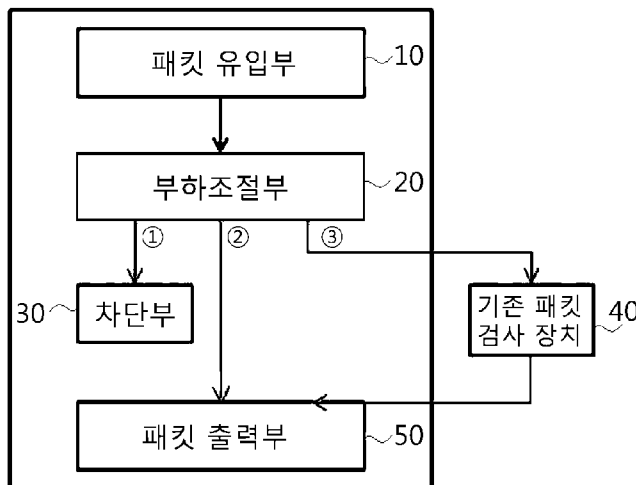
- 국제조사보고서와 함께 (조약 제 21 조(3))

[다음 쪽 계속]

(54) Title: METHOD AND APPARATUS FOR ADJUSTING LOAD OF PACKET INSPECTION DEVICE

(54) 발명의 명칭 : 패킷검사장치의 부하조절방법 및 장치

[Fig. 2]



- 10 ... Packet entering unit
20 ... Load adjusting unit
30 ... Blocking unit
40 ... Existing packet inspection device
50 ... Packet outputting unit

(57) Abstract: The present invention is to prevent a packet inspection device from stopping the operation of the packet inspection device when a load applied to the packet inspection device is larger than the maximum capacity that the packet inspection device can handle. A method and an apparatus for adjusting a load according to the present invention can ensure that the packet inspection device keeps working even in case of overload by periodically monitoring the amount of packets, that is, load levels, entering into the packet inspection device, and by comparing the monitored load levels with the predetermined upper and lower limits, in order to pass the packets through the packet inspection device or to block some of the packets if the load levels exceed a certain value. In addition, the method and the apparatus for adjusting a load according to the present invention are simply configured to effectively select the packets to be blocked or passed in order to not damage the unique functions of the packet inspection device, and to prevent another load from being induced during the selecting procedure. Further, the apparatus for adjusting a load selectively operates only in case an overload has been generated.

(57) 요약서:

[다음 쪽 계속]



본 발명은 패킷검사장치로 유입되는 부하가 패킷검사장치가 처리할 수 있는 최대 용량보다 클 때 패킷검사장치가 동작을 멈추게 되는 현상을 방지하기 위한 것이다. 본 발명에 따른 부하조절방법 및 장치는 패킷검사장치로 유입되는 패킷의 양, 즉 부하 수준을 주기적으로 모니터링하면서 미리 정해진 상한값과 하한값과 비교하여, 부하 수준이 일정한 값을 넘을 때는 패킷의 일부를 차단하거나 혹은 패킷검사장치를 통과하도록 함으로써 과부하 상태에서도 패킷검사장치가 계속 동작할 수 보장한다. 또한 본 발명에서의 부하조절방법 및 장치는 패킷검사장치의 고유 기능을 훼손하지 않도록 차단시키거나 통과시킬 패킷을 효과적으로 선별하고, 선별 과정이 별도의 부하를 다시 유발하지 않도록 간단하게 구성되며, 과부하에 해당될 경우에만 부하조절장치가 선택적으로 동작하는 것을 특징으로 한다.

명세서

패킷검사장치의 부하조절방법 및 장치

기술분야

- [1] 본 발명은 서비스거부 공격에 대한 생존성을 향상시키기 위하여 패킷검사장치의 부하를 조절하는 방법 및 장치에 관한 것으로, 보다 상세하게는 서비스거부 공격에 의하여 다량의 패킷들이 패킷검사장치에 유입되면 패킷검사장치로 패킷들이 전달되기 전에, 간단한 조건을 이용하여 패킷들을 우선 분류하고 분류한 일부 패킷들을 자체적으로 차단하거나 혹은 기존 패킷검사장치를 통과하도록 하여 패킷검사장치의 부하가 일정 수준을 넘지 않게 하는 방법에 관한 것이다.

[2]

배경기술

- [3] 서비스거부 공격(Denial of Service Attack)은 다수의 좀비 시스템으로 공격하는 분산 서비스거부 공격(Distributed Denial of Service Attack)과 단일 시스템으로 인터넷 프로토콜의 취약점이나 시스템의 취약점을 이용하는 공격으로 나뉜다. 다수의 좀비 컴퓨터로 이루어지는 분산 서비스거부 공격은 여러 대의 좀비 시스템이 한 대의 시스템을 공격하는 형태이다. 이러한 분산 서비스거부 공격은 취약점을 이용하지 않고 정상적인 서비스 요청으로도 공격이 가능하다. 최근에는 이러한 정상적인 서비스 요청을 이용한 공격이 늘어나고 있어 패킷검사장치(시스템 보안장비)가 정상적인 서비스 요청과 악의적인 서비스 요청을 구별하는데 어려움을 겪고 있다.
- [4] 종래 서비스거부 공격을 탐지하는 방법에 의하면, 패킷을 일일이 규칙과 비교하여 검사하기 때문에 과정이 복잡하다. 이때 패킷을 검사하는데 사용되는 규칙은 크게 패킷의 헤더(header)를 검사하는 것과 패킷의 내용, 즉 페이로드(payload)를 검사하는 것으로 구분된다. 페이로드를 검사하는 규칙을 적용하기 위한 과정이 일반적으로 훨씬 복잡하다. 예를 들어 패킷의 페이로드 전체에서 'attack' 문자열이 있으면 공격으로 판단하는 규칙이 있다면, 페이로드 전체를 순차적으로 검사해서 'attack' 문자열의 존재 여부를 판단하여야 하므로 페이로드가 길수록 그리고 검사해야 하는 규칙의 수가 증가할수록 검사 과정은 더욱 복잡해진다. 따라서 서비스거부 공격에 의하여 다량의 패킷이 한꺼번에 시스템으로 유입될 경우 정상적인 패킷들의 처리 시간도 길어져서 오히려 공격의 효과를 증대시키는 역효과를 발생시킬 수 있다.

[5]

발명의 상세한 설명

기술적 과제

- [6] 본 발명은 전술한 기존 패킷검사장치(시스템 보안장비)의 취약점을 보완하기

위한 것으로, 과부하일 경우 패킷검사장치로 유입되는 패킷의 양을 선제적으로 조절하되 차단해야 할 패킷과 검사가 필요없는 패킷들을 구분함으로써 패킷검사장치를 포함한 시스템의 기능을 유지하면서도 패킷검사장치가 실질적으로 처리해야 하는 부하를 경감시키고, 이를 통하여 서비스 거부 공격으로 인한 시스템 동작 중지를 예방하며 나아가 시스템의 생존성을 향상시킴과 동시에 정상 패킷들의 서비스 대기 시간을 줄일 수 있는 방법 및 장치를 제공하는 것을 목적으로 한다.

- [7] 종래의 방법 또는 본 발명에서 인용하는 기존 패킷검사장치는 자세한 패킷 검사로 인하여 대량의 패킷이 한꺼번에 유입될 때 처리할 수 있는 패킷의 수에 대한 제약이 있다. 이 때 처리될 수 없는 패킷들은 임의로 폐기되거나 심지어 패킷검사장치의 동작이 멈추는 현상이 발생되는데, 본 발명에 의한 부하조절장치는 이런 문제점을 해결하기 위한 것이다.

[8]

기술적 해결방법

- [9] 전술한 목적을 달성하기 위한 본 발명에 의한 방법 및 장치는, (A) 패킷검사장치로 유입되는 패킷의 양을 측정하여 패킷검사장치가 처리할 수 있는 상한값이나 하한값과 비교하는 단계; (B) ① 유입량이 상한값 이하이면 유입되는 패킷을 패킷검사장치로 전달하고, 즉 부하조절장치를 동작시키지 않고, ② 유입량이 상한값을 초과하면, 각 패킷에 대하여 헤더 정보만을 이용하여 차단 대상 여부와 통과 대상 여부를 결정한 후에 차단 대상일 경우 폐기시키고, 통과 대상일 경우 상기 패킷검사장치를 통과시키고, 그렇지 않은 경우에만 패킷검사장치로 전달하는 단계;를 반복 수행하는 부하조절방법에 관한 것이다. 본 발명에서 상기 패킷 검사장치는 종래 알려진 검사장치를 배제하지 않는다.
- [10] 본 발명에서의 상기 단계 (B)에서 차단 대상 여부와 통과 대상 여부를 결정하는 방법은 패킷의 헤더만을 이용한다는 점에서 패킷의 내용까지 검사하는 일반적인 방법에 비하여 매우 간단하므로 패킷검사장치에 패킷을 전달하기 전에 선제적인 방법으로 사용하기에 적합하다. 또한 패킷의 헤더에서 추출한 정보로부터 생성한 수치를 활용하므로 차단 대상 혹은 통과 대상을 결정하는 과정이 단순하다.
- [11] 또한 본 발명의 상기 단계 (B)에서는, 유입되는 패킷의 양이 유동적으로 변하는 반면 패킷검사장치가 처리할 수 있는 용량은 일정하다는 점에서 차단 대상 여부와 통과 대상 여부를 판단하기 위한 차단 임계값과 통과 임계값의 크기를 유입 부하에 연동하여, 즉 피드백을 통하여 조절하는 것이 바람직하다.

[12]

유리한 효과

- [13] 본 발명을 기존의 패킷검사장치에 앞서서 선제적으로 적용하면 기존의 패킷검사장치를 그대로 활용하면서도 패킷검사로 인한 과부하를 방지하고

서비스 거부 공격 효과를 경감시킬 수 있고, 이를 통하여 시스템의 전체 부하가 작아지므로 시스템의 생존성을 증대시킬 수 있다.

- [14] 또한 본 발명에 의하면, 패킷검사장치에 의한 검사를 생략하고 통과되는 패킷들은 검사로 인한 지연시간이 없기 때문에 서비스 대기 시간을 단축시키는 효과도 있다.

[15]

도면의 간단한 설명

- [16] 도 1은 본 발명에 의한 부하조절방법에 따라 유입된 패킷들의 분류 형태를 도식적으로 표현한 개념도.

- [17] 도 2는 종래 서비스거부 공격 방지 시스템에 본 발명에 의한 부하조절방법을 수행하는 부하조절부가 추가된 시스템의 예시적 개념도.

- [18] 도 3은 부하조절부의 기능별 구조를 상세하게 예시한 개념도.

- [19] 도 4는 선택적 흐름변경 스위치의 동작을 설명하는 순서도.

- [20] 도 5는 패킷분류부의 동작을 설명하는 순서도.

[21]

- [22] <도면 중 주요부분에 대한 설명>

- [23] 10 : 패킷유입부 20 : 부하조절부

- [24] 30 : 차단부 40 : 패킷검사장치

- [25] 50 : 패킷출력부

- [26] 201 : 스위치 202 : 패킷분류부

[27]

발명의 실시를 위한 최선의 형태

- [28] 본 발명은 패킷검사장치에 유입되는 부하의 양을 조절하기 위한 것이다.

패킷의 흐름 관점에서 보면 본 발명에 의한 부하조절장치는 기존의 패킷검사장치에 앞서 설치되며, 기존의 패킷검사장치의 과부하가 의심될 때만 부하조절장치가 선택적으로 동작한다. 즉 패킷검사장치에 인가되는 부하가 지나치게 클 때만 부하조절장치가 동작하고, 그렇지 않은 경우에는 부하조절장치는 모든 패킷을 패킷검사장치로 그대로 전달하게 된다.

- [29] 본 발명은 시스템의 부하가 커지면 간단한 조건을 사용하여 의심스런 패킷들과 안전한 패킷들을 분류하고, 이렇게 분류된 일부 패킷을 패킷검사장치에 도달하지 못하도록 차단하거나 기존 패킷검사장치에서 검사하지 않도록 통과시킴으로써 패킷검사장치에 인가되는 부하의 크기가 일정 범위를 넘지 않도록 조절한다. 결과적으로 시스템의 생존성은 향상되고 정상 패킷들의 서비스 대기 시간은 줄어드는 효과를 얻을 수 있다.

- [30] 본 발명에서는 패킷검사장치에 유입되는 부하의 크기를 측정하기 위하여 초당 패킷의 수, PPS(Packets Per Second)를 사용한다. 지금부터 부하조절장치에 유입되는 모든 패킷은 '유입 패킷량(PPS_{in})', 부하조절장치를 거쳐서 기존의

패킷검사장치로 전달되는 패킷의 양은 '부하 패킷량(PPS_{load})', 기존의 패킷검사장치가 처리할 수 있는 최대 패킷 처리량은 ' PPS_{high} ', 비정상 패킷을 구분하여 제한할 필요가 없을 만큼 충분히 작은 패킷 처리량은 ' PPS_{low} ', 유해하다고 판단되어 차단되는 패킷의 양은 '차단 패킷양(PPS_{block})', 무해하다고 판단되어 패킷검사장치에서의 검사없이 통과되는 패킷은 '통과 패킷양(PPS_{bypass})'으로 표기한다.

- [31] 본 발명에서의 부하조절장치가 없을 때는 패킷검사장치에 대한 PPS_{load} 은 PPS_{in} 과 같다. 즉, 부하조절장치에 유입된 모든 패킷이 그대로 패킷검사장치로 전달된다. 패킷검사장치의 과부하가 예상되면, 즉 $PPS_{in} > PPS_{high}$ 로 측정되면, 부하조절장치가 동작함으로써 PPS_{load} 를 PPS_{high} 보다 낮춰서 패킷검사장치의 부하를 줄이고, 과부하 상태가 해소되면 즉, PPS_{load} 가 PPS_{low} 보다 작아지면 부하조절장치의 동작을 중지시킴으로써 PPS_{load} 가 다시 PPS_{in} 과 같아진다.

[32]

- [33] 이하 첨부된 도면을 참조하여 본 발명을 보다 상세히 설명한다. 첨부된 도면들은 본 발명에 의한 부하조절방법을 수행할 수 있는 장치, 즉 부하조절장치에 관한 것이다. 예시적 장치를 가정하고 본 발명에 의한 부하조절방법의 구체적 내용을 설명한다. 그러나 이러한 도면 및 그에 대한 설명은 본 발명의 기술적 사상의 내용과 범위를 쉽게 설명하기 위한 예시일 뿐, 이에 의해 본 발명의 기술적 범위가 한정되거나 변경되는 것은 아니다. 또한 이러한 예시에 기초하여 본 발명의 기술적 사상의 범위 안에서 다양한 변형과 변경이 가능함은 당업자에게는 당연할 것이다.

- [34] 본 발명에서 '잠재적 유해성' 또는 '잠재적 무해성'이란 패킷검사장치에 의한 정밀검사(통상의 검사) 이전에 패킷의 헤더 정보만을 사용하는 간단한 기준에 따라 일차적으로 패킷을 분석한 결과, '정밀검사하면 유해성으로 판단될 가능성이 높음' 또는 '정밀검사하면 무해성으로 판단될 가능성이 높음'을 의미한다.

[35]

- [36] 도 1은 본 발명에 의한 검사방법에 따라 유입된 패킷들이 소정의 기준에 따라 분류되어 일부는 차단되고, 일부는 통과되고, 나머지 패킷들만 패킷검사장치로 전달되어 정밀검사되는 과정을 도식적으로 표현한 개념도이다.

- [37] 서비스 거부 공격이 발생 되면(보다 정확하게는, 패킷검사장치의 최대 패킷 처리량보다 많은 양의 패킷의 유입되면) PPS_{in} 에 해당하는 패킷들에 대하여 간단한 조건으로 패킷의 잠재적 유해성을 측정하고, 이를 기준으로 패킷을 분류하여 잠재적으로 유해한 것으로 판단되는 패킷은 차단하고 잠재적으로 무해한 것으로 판단되는 패킷은 패킷검사장치를 통과시킨다. 그 외의 패킷들, 즉 잠재적 유해성이나 잠재적 무해성에 대한 판단이 유보된 패킷들은 정밀검사를 위하여 기존의 패킷검사장치로 전달되는데, 그 양이 PPS_{high} 를 넘지 않도록 잠재적 유해성 혹은 잠재적 무해성을 판단하기 위한 기준을 동적으로 변경한다.

이 때 잠재적 유해성 혹은 잠재적 무해성에 대한 판단 기준은 차단 임계값 혹은 통과 임계값이 되므로 임계값을 변경함으로써 잠재적 유해성 혹은 잠재적 무해성을 판단하기 위한 기준을 변경할 수 있다.

[38]

[39] 차단 임계값 혹은 통과 임계값은 잠재적 유해성 혹은 잠재적 무해성을 판단하기 위한 기준이다. 본 발명에 의한 부하조절방법 및 장치는 기존의 패킷검사장치에 앞서서 선제적으로 패킷의 일부를 분류해내는 것을 목적으로 한다는 점에서 잠재적 유해성 혹은 잠재적 무해성에 해당되는 패킷의 양을 최소한도로 억제하는 것이 바람직하다. 본 발명에서 제시되는 방법은 이런 목적을 달성하기 위하여 차단 임계값과 통과 임계값을 다음과 같이 동적으로 조절한다.

[40]

부하조절장치가 동작을 시작하면 미리 정해진 값으로 차단 임계값과 통과 임계값을 설정한다. 부하조절장치에 의하여 패킷검사장치로 전달되는 패킷의 양, 즉 PPS_{load} 가 여전히 PPS_{high} 보다 크면 차단 임계값과 통과 임계값을 변경하여 PPS_{load} 가 작아지도록 조절한다. 반면에 PPS_{load} 가 PPS_{high} 보다 너무 작아지면 차단 임계값과 통과 임계값을 변경하여 PPS_{load} 가 커지도록 조절함으로써 불필요하게 차단되거나 통과되는 패킷을 최소화한다. 즉, 부하조절장치에 의한 PPS_{load} 를 피드백받아서 PPS_{high} 와 비교하고 이를 토대로 부하조절장치에 의한 PPS_{load} 가 PPS_{high} 를 넘지 않도록 가능하면 큰 값을 유지할 수 있도록 제어한다.

[41]

[42] 이 때 패킷의 잠재적 유해성과 잠재적 무해성에 대한 판단은 패킷 헤더 정보에 의존하며 판단 절차가 간단하여 처리시간이 짧아야 한다. 서비스거부 공격에서 잘 나타나는 특징이 잠재적 유해성을 판단하는데 활용되며, 서비스거부 공격에서 잘 나타나지 않는 특징은 잠재적 무해성을 판단하는데 활용될 수 있다.

[43]

잠재적 유해성 판단 방법에 대한 예시는 다음과 같다. 패킷 헤더에서 추출한 송신지 IP 주소와 수신지 IP 주소 정보를 이용하여 송신자와 수신자에 대한 집중도를 수치화한다. 특정 호스트를 공격함으로써 서비스거부를 유발하는 상황에서는 수신지 IP 주소가 특정 주소로 집중될 수밖에 없다. 따라서 패킷을 받을 때마다 수신지 IP 주소를 추출하여 단위시간 동안의 수신지 IP 주소의 집중도를 수치화하고, 이 정보를 이용하여 서비스거부 공격에 대한 가능성을 유추하면 잠재적 유해성 여부를 판단할 수 있다. 한편 잠재적 유해성 검사를 통과한 패킷들, 즉 유해하지 않은 것으로 판단된 패킷들에 대해서 송신지 IP 주소의 집중도를 수치화하여 집중도가 높은 송신지에서 발송된 패킷들을 잠재적으로 무해하다고 판단한다. 이는 유해한 패킷들이 배제된 이후에 중복되는 송신자는 네트워크 장애 혹은 서비스 필요성 때문에 패킷을 다량으로 발송하는 것으로 추정해도 무방하기 때문이다.

[44]

[45] 도 2는 종래 서비스거부 공격을 방지하기 위한 패킷검사장치에 본 발명에 의한

부하조절방법을 수행하는 부하조절부(20)가 추가된 시스템의 예시적 개념도이다. 패킷유입부(10)를 통하여 유입된 패킷은 패킷출력부(50)를 거쳐서 나간다. 종래 방법(모든 유입 패킷을 일일이 정밀검사하는 방법)에 의한 패킷검사장치 앞에 본 발명을 수행하는 부하조절부(20)를 추가함으로써 유입되는 패킷이 일정 수준을 넘을 때는 부하조절부(20)에서 일부 패킷을 차단하거나 통과시키고 기존 패킷검사장치가 처리할 수 있는 범위 내의 패킷의 양만 기존 패킷검사장치로 보낸다. 기존 패킷 검사장치(40)에서는 통상의 방법으로 정밀하게 패킷을 검사하고 유해한 것으로 판정된 패킷만을 차단한다. 차단부(30)에 전달된 패킷은 모두 폐기되는데, 이러한 기능은 물리적으로 독립될 필요는 없고 부하조절부(20)의 세부 기능 중 하나가 될 수도 있다.

[46]

[47] 도 3은 부하조절부(20)의 기능별 구조를 상세하게 예시한 개념도로서, 시스템의 현재 부하를 측정하여 패킷의 흐름을 변경시키는 선택적 흐름변경 스위치(201)와 기존 패킷검사장치(40)의 부하에 따라서 패킷의 양을 조절하여 패킷검사장치로 전달되는 부하를 줄이기 위한 패킷분류부(202)로 구성될 수 있다.

[48]

선택적 흐름변경 스위치(201)는 시스템이 과부하 상태이면 패킷을 패킷분류부(202)로 보내고 정상부하 상태이면 기존 패킷검사장치(40)로 보내는 역할을 한다. 패킷분류부(202)는 차단 임계값과 통과 임계값을 이용하여 차단할 패킷(①), 기존 패킷검사장치(40)를 통과시킬 패킷(②), 그리고 기존 패킷검사장치(40)로 하여금 정밀검사할 패킷들(③)로 구분한다. 패킷 분류부에서 기존 패킷검사장치(40)로 보내는 패킷은 선택적 흐름변경 스위치(201)가 정상부하 상태인 경우의 모든 패킷과 같이 기존 패킷검사장치(40)로 전달된다. 도면에서 A 부분은 이러한 두 가지 경우를 합치는 역할을 하는데, 이러한 기능은 반드시 존재해야 하는 것은 아니다. 도 3에서는 이해의 편의를 위하여 유입되는 패킷 경로와 유출되는 패킷 경로에 패킷의 양을 표현하는 PPS_{in} , PPS_{block} , PPS_{bypass} , PPS_{load} 을 부기하였다.

[49]

[50] 도 4는 도 2 및 도 3에서 언급된 선택적 흐름변경 스위치(201)의 동작을 설명하는 예시적 순서도이다. 선택적 흐름변경 스위치(201)는 PPS_{in} 을 측정하고 현재 과부하 상태 여부를 참고하여 PPS_{high} 또는 PPS_{low} 와 비교한 후 필요할 경우 스위치 상태를 변경한다. 즉, 선택적 흐름변경 스위치(201)의 현재 위치가 '과부하 상태'라면 PPS_{in} 이 PPS_{low} 이하로 내려갈 때 '정상부하 상태'로 스위치를 변경하고 흐름 변경 스위치의 현재 위치가 '정상부하 상태'라면 유입 패킷량(PPS_{in})이 PPS_{high} 보다 올라갈 때 '과부하 상태'로 스위치를 변경한다.

[51]

과부하 상태로 스위치를 변경할 때는 패킷분류부(202)에서 사용될 차단임계값과 통과임계값을 초기화한다. 차단임계값과 통과임계값의 초기값은 패킷검사장치에 전달되는 패킷량을 충분히 줄일 수 있는 값을 선택한다.

[52]

[53] 도 5는 패킷분류부(202)의 동작을 설명하는 예시적 순서도이다.

패킷분류부(202)에서는 패킷 헤더로부터 계산된 '패킷의 잠재적 유해성 수치'가 차단임계값 이상일 경우 상기 패킷을 '차단'하고, '패킷의 잠재적 무해성 수치'가 통과임계값 이상일 경우 상기 패킷을 '통과'시킨다. 두 조건에 모두 해당되지 않는 경우에만 패킷검사장치(40)로 전달하여 '검사'받도록 한다. 이해의 편의를 위하여 도 5에서의 ①, ②, ③은 도 3에서의 ①, ②, ③과 일치하도록 표시하였다.

[54]

한편, 패킷분류부(202)가 효과적으로 동작하기 위하여 부하조절부(20)는 차단임계값과 통과임계값을 동적으로 변경하기 위한 기능을 갖는다.

패킷검사장치(40)로 전달되는 패킷의 양, PPS_{load} 을 피드백 받아서 PPS_{high} 와 비교한 후, PPS_{load} 가 PPS_{high} 를 넘지 않는 범위에서 가능한 큰 값이 되도록 차단임계값과 통과임계값을 유기적으로 변경하여야 한다. 차단임계값과 통과임계값은 기본적으로 패킷의 수를 표시한다. 앞에서 설명한 것처럼 송신지 IP 주소가 중복될 경우 서비스거부 공격으로 의심되므로 해당되는 패킷을 차단할 필요가 있는데, 차단에 필요한 패킷의 중복 정도를 표시하기 위한 것이 차단임계값이며, 같은 방법으로 통과에 필요한 패킷의 중복 정도를 표시하기 위한 것이 통과임계값이다. 차단임계값과 통과임계값을 동적으로 변경하기 위한 공식은 다음과 같다.

[55]

$$Th_{new} = \alpha \cdot \gamma \cdot Th_{old} + (1 - \alpha)Th_{old}$$

[56]

Th_{old} 와 Th_{new} 는 변경전의 임계값과 변경후의 임계값을 나타내며, γ 는 임계값을 갱신하기 위한 계수이다. γ 를 계산하기 위한 방법중의 하나는 PPS_{high} 와 PPS_{load} 의 비,

$$\frac{PPS_{high}}{PPS_{load}}$$

를 구하는 것이다. PPS_{high} 가 PPS_{load} 보다 크면 γ 가 1보다 커지므로 임계값은 증가하는데, 이것은 차단이나 통과로 판단할 가능성이 감소했다는 것을 의미한다 (임계값보다 큰 경우에만 차단되거나 통과된다). PPS_{load} 의 값이 PPS_{high} 보다는 작아야 하지만 가능한 큰 값을 취해야 한다는 점에서 PPS_{load} 를 증가시키는 효과를 가져온다. 한편 PPS_{high} 가 PPS_{load} 보다 작으면, 즉 과부하 상태이면 γ 가 1보다 작게 되므로 임계값이 감소하고, 이것은 차단이나 통과시킬 패킷의 수를 증가시킴으로써 패킷검사장치에 인가되는 부하인 PPS_{load} 의 감소를 가져온다.

[57]

α 는 임계값을 얼마나 신속하게 변경하는가에 관한 정도를 조절하기 위한 것이다. α 가 1이면 이전의 임계값 Th_{old} 을 이후의 임계값 $\gamma \cdot Th_{old}$ 로 바로 변경한다는 것을 의미하지만 α 가 0에 가까워질수록 새로운 임계값을 반영하는 정도가 작아지므로 점진적으로 임계값이 변화하게 된다. α 가 크면 클수록 부하를 단시간에 조절할 수 있지만, 적절한 임계값으로 수렴하는 과정에서

일종의 진동이 나타나게 된다. 반면 α 를 작게 하면 인가되는 부하의 양이 급격하게 증가하거나 감소할 때 이에 대응하는데 소요되는 시간은 더 걸리게 되지만 전체적인 부하조절 기능은 개선되는 효과를 기대할 수 있다.

[58]

[59] 한편 잠재적 유해성과 잠재적 무해성을 판단하는 기준에는 앞에서 설명한 송신지 IP 주소와 수신지 IP 주소 외에도 패킷의 길이 등 패킷 헤더로부터 얻을 수 있는 다른 정보를 활용할 수도 있다. 일반적으로 서비스거부 공격을 유발하는 패킷들의 길이는 짧기 때문에, 패킷의 길이를 임계값으로 활용하여 임계값보다 긴 패킷은 잠재적으로 무해하다고 추측할 수 있다. 즉, 잠재적으로 무해하다고 판별해야 하는 패킷의 수를 늘려야 할 필요가 있으면 임계값을 낮춤으로써 더 많은 패킷이 잠재적으로 무해한 것으로 판별되도록 하고, 반대의 경우에는 임계값을 높임으로써 무해한 것으로 판별되는 패킷의 수를 줄인다.

[60]

산업상 이용가능성

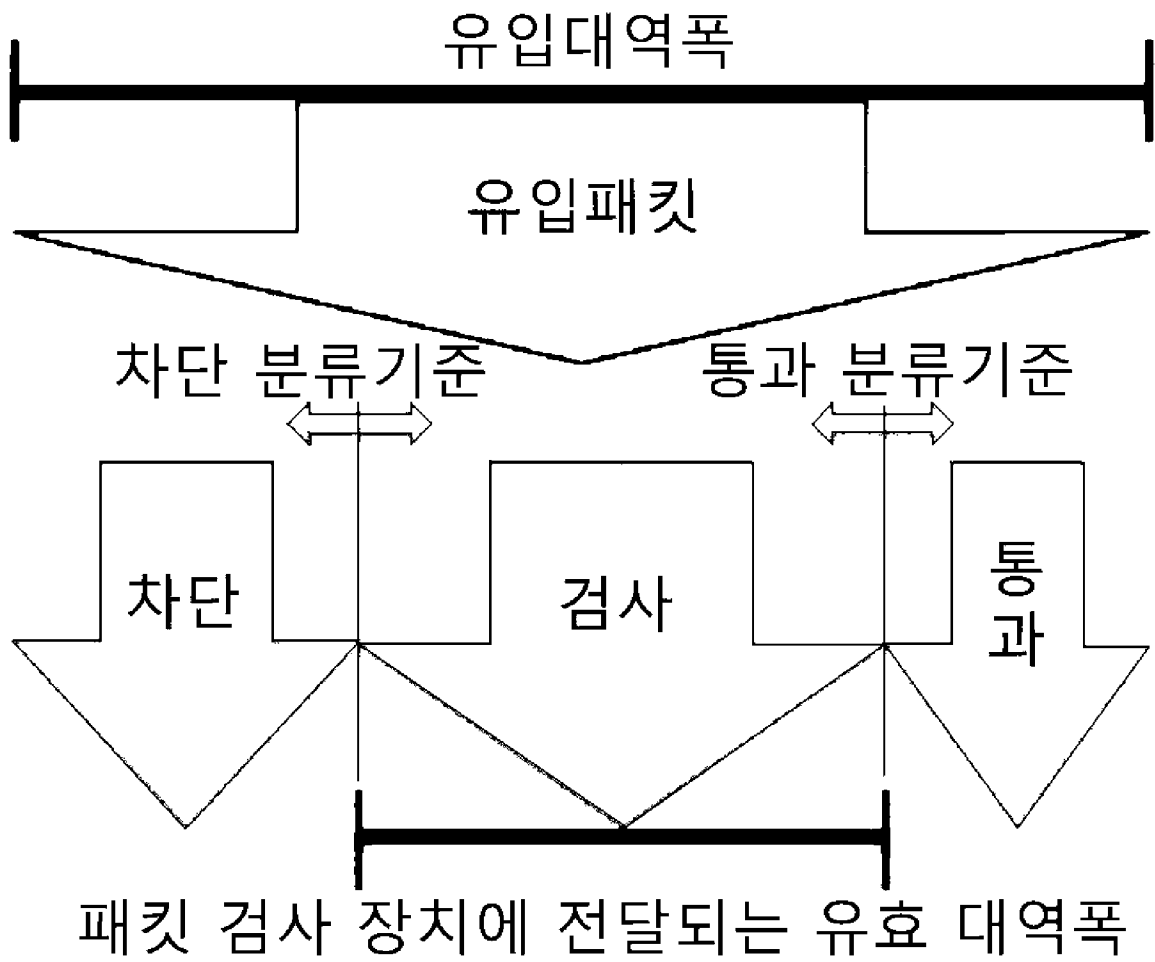
[61] 본 발명의 패킷검사장치의 부하 조절 방법 및 장치에 의해 기존의 패킷검사장치에 패킷이 유입되기 전에 패킷을 우선 분류하고 분류한 패킷들을 자체적으로 차단하거나 패킷검사장치를 통과하도록 하는 것에 의해 패킷검사로 인한 과부하를 방지하고 서비스 거부 공격 효과를 경감시킬 수 있다.

[62] 또한, 패킷검사장치에 의한 검사를 생략하고 통과되는 패킷들은 검사로 인한 지연시간이 없기 때문에 서비스 대기 시간을 단축시킬 수 있다.

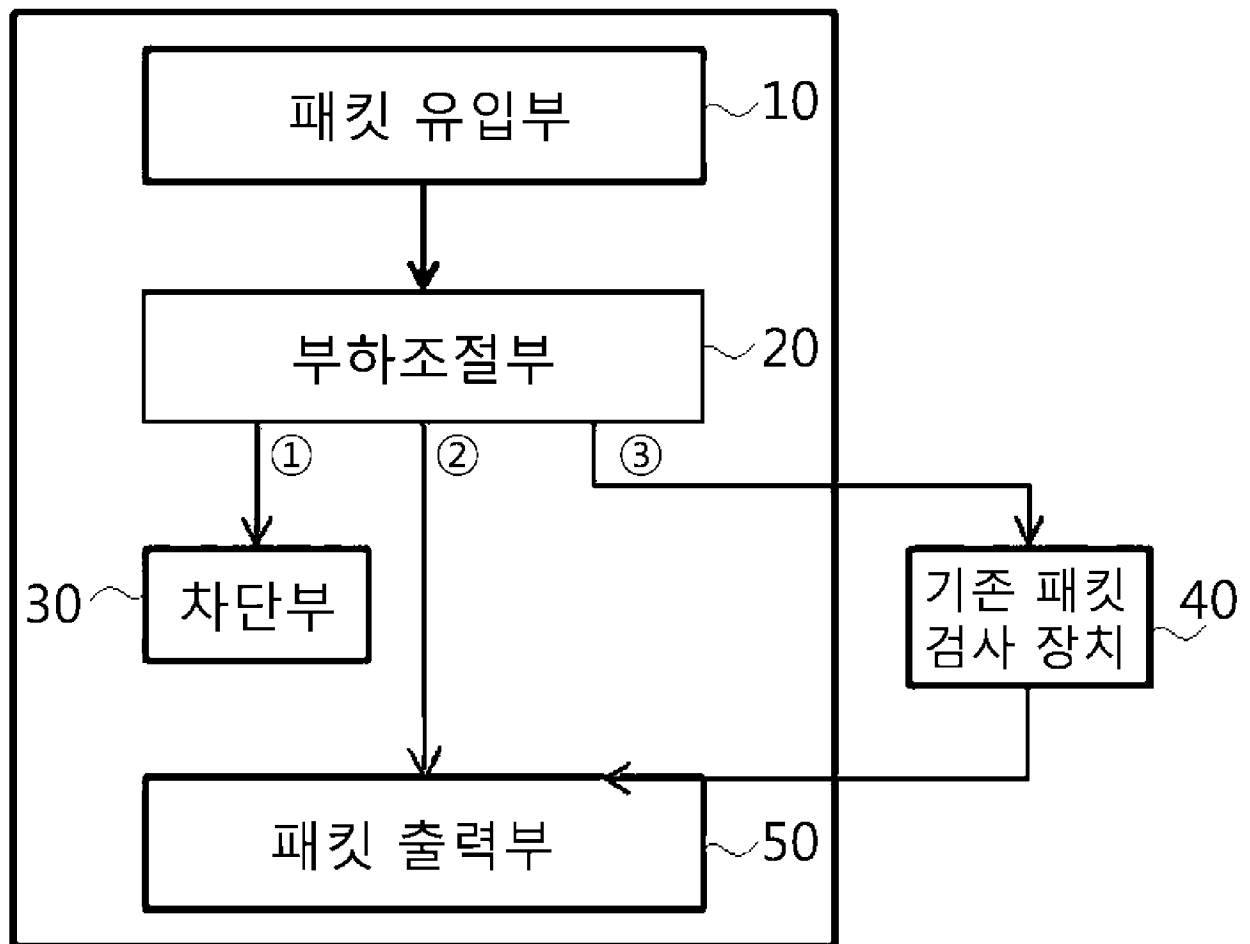
청구범위

- [1] (A) 패킷검사장치로 유입되는 패킷의 양을 측정하여 패킷검사장치가 처리할 수 있는 상한값이나 하한값과 비교하는 단계;
 (B) ① 유입량이 상한값 이하이면 유입되는 패킷을 패킷검사장치로 전달하고, 즉 부하조절장치를 동작시키지 않고, ② 유입량이 상한값을 초과하면, 각 패킷에 대하여 헤더 정보만을 이용하여 차단 대상 여부와 통과 대상 여부를 결정한 후에 차단 대상일 경우 폐기시키고, 통과 대상일 경우 상기 패킷검사장치를 통과시키고, 그렇지 않은 경우에만 패킷검사장치로 전달하는 단계;
 를 반복 수행하는 것을 특징으로 하는 부하조절방법.
- [2] 제 1 항에 있어서,
 상기 단계 (B)에 있어서, 패킷 헤더에서 송신지 IP 주소 혹은 수신지 IP 주소를 추출하여 단위시간 동안 누적된 정보를 이용하여 패킷의 집중도를 측정하고 이를 이용하여 잠재적 유해성 혹은 잠재적 무해성을 판단하는 부하조절방법.
- [3] 제 2 항에 있어서,
 수신지 IP 주소의 집중도에 대한 수치가 차단임계값보다 클 경우 잠재적으로 유해하다고 판단하고, 송신지 IP 주소의 집중도에 대한 수치가 통과임계값보다 클 경우 잠재적으로 무해하다고 판단하는 부하조절방법.
- [4] 제 3 항에 있어서,
 패킷검사장치에 전달되는 패킷의 양을 피드백 받아서 패킷검사장치의 부하 수준이 일정 수준 이하에서 가능한 최대값을 유지하도록 차단임계값과 통과임계값을 동적으로 변경하는 것을 특징으로 하는 부하조절방법.

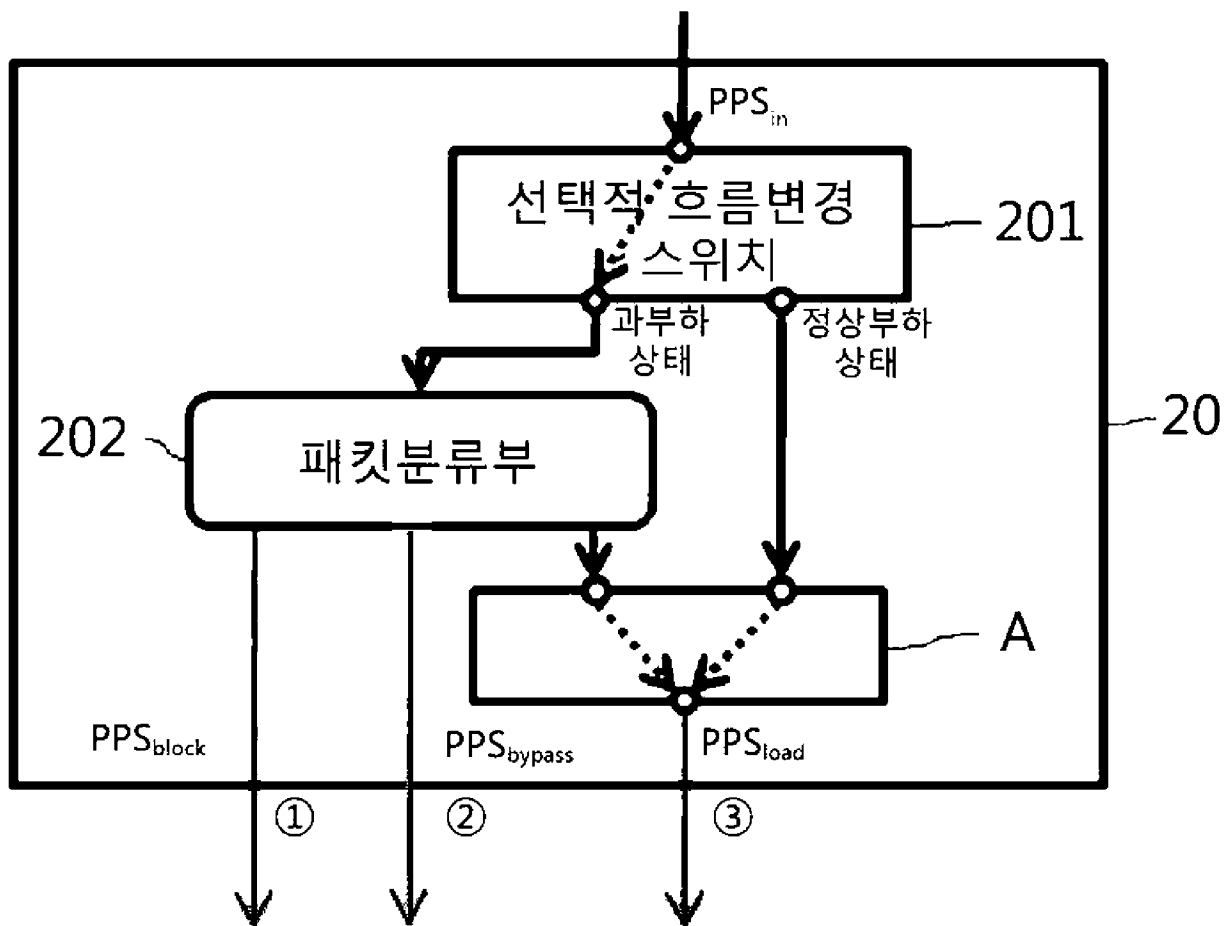
[Fig. 1]



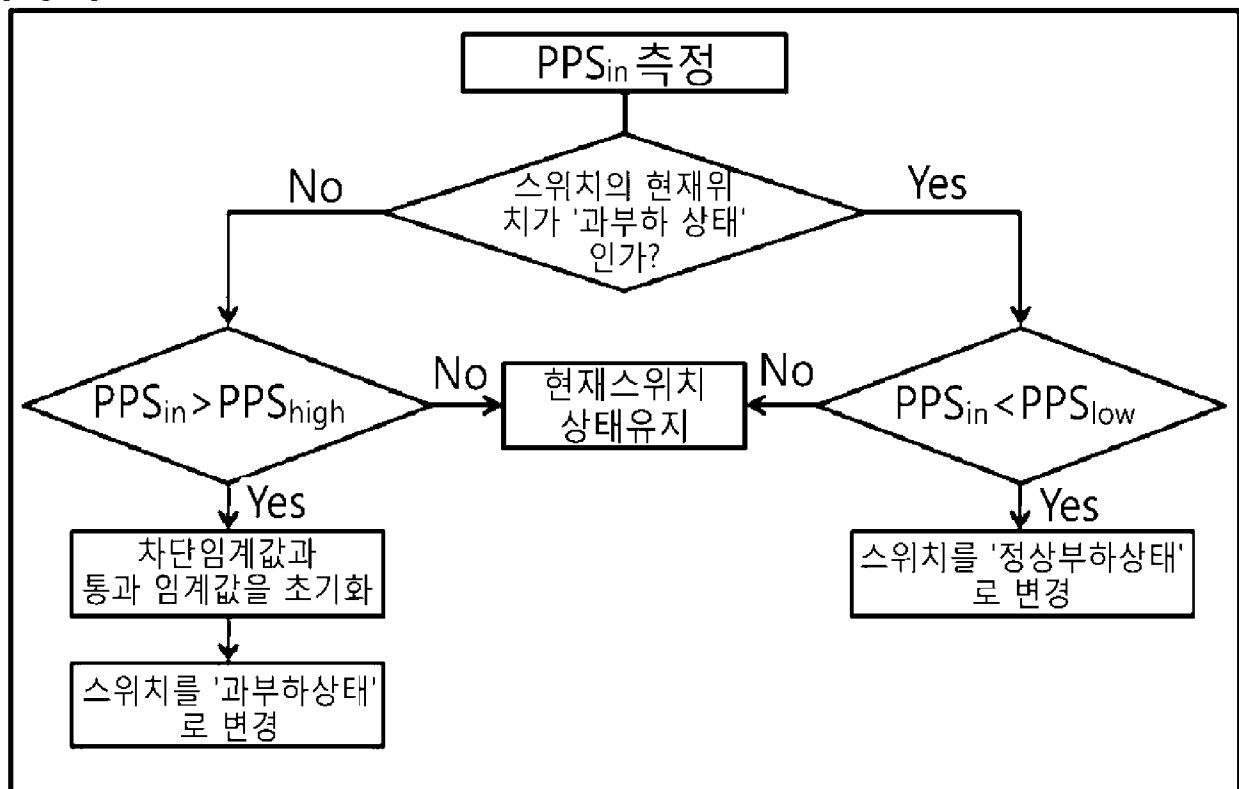
[Fig. 2]



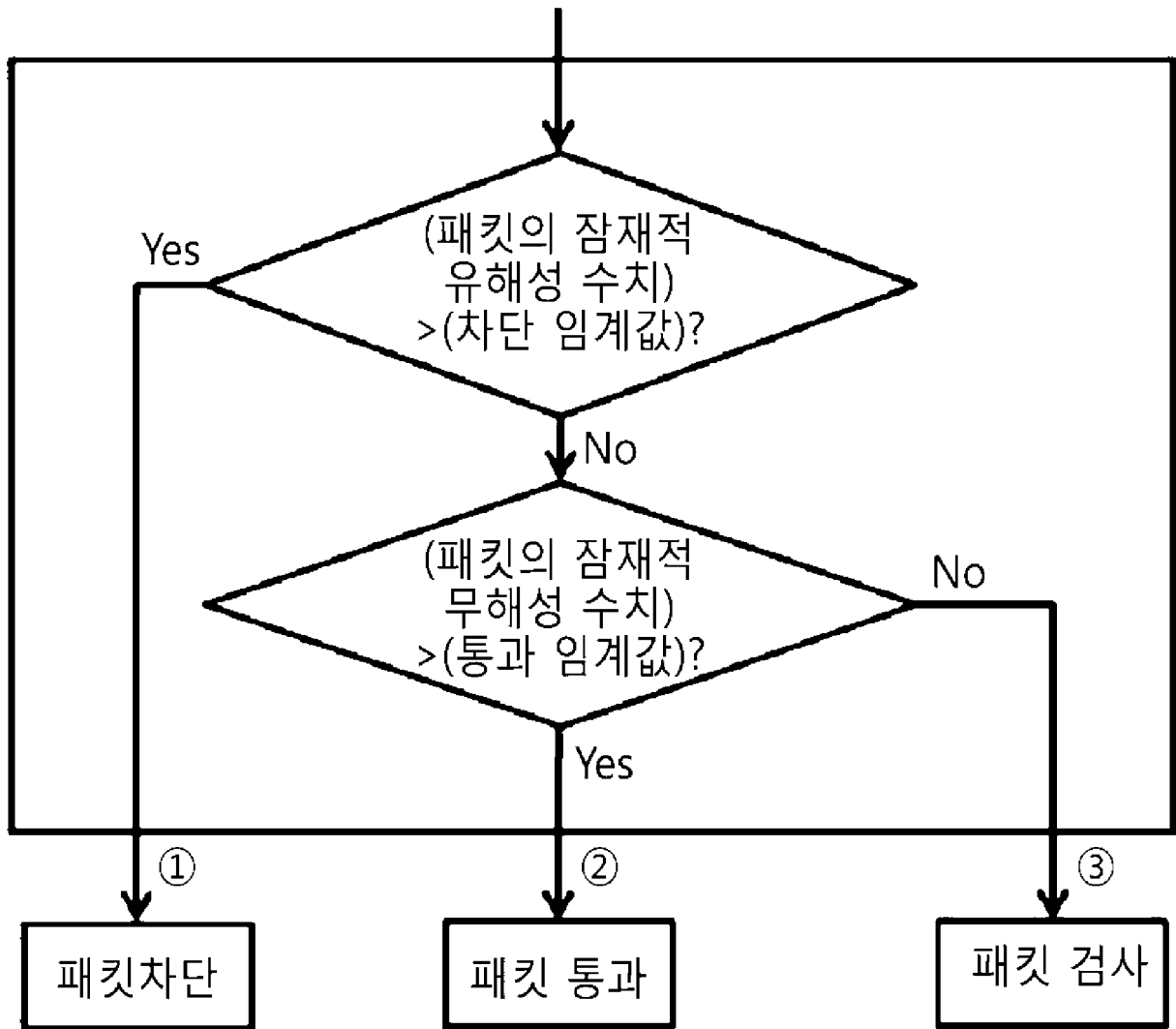
[Fig. 3]



[Fig. 4]



[Fig. 5]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2009/003693**A. CLASSIFICATION OF SUBJECT MATTER****H04L 12/26(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 12/26; G06F 17/00; H04L 12/22; H04L 12/28; H04L 9/32

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: Denial of Service Attack, on the fly packet, load balancing, filtering

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2009-0044177 A (DASAN NETWORKS, INC.) 07 May 2009 See the entire document	1-4
A	KR 10-2004-0074367 A (LGNSYS INC.) 25 August 2004 See the entire document	1-4
A	KR 10-2003-0059204 A (WANWALL INC.) 07 July 2003 See the entire document	1-4
A	KR 10-2005-0010896 A (THOMSON LICENSING) 28 January 2005 See the entire document	1-4



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

27 JULY 2010 (27.07.2010)

Date of mailing of the international search report

27 JULY 2010 (27.07.2010)

Name and mailing address of the ISA/

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/KR2009/003693

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 10-2009-0044177 A	07.05.2009	NONE	
KR 10-2004-0074367 A	25.08.2004	NONE	
KR 10-2003-0059204 A	07.07.2003	AU 2002-13264 A1	29.04.2002
		AU 2002-213264 A8	29.04.2002
		AU 2002-360197 A1	23.06.2003
		AU 2002-360197 B2	21.08.2008
		CA 2469885-A1	19.06.2003
		CN 101242415 A	13.08.2008
		CN 101242415 C0	13.08.2008
		CN 101242416 A	13.08.2008
		CN 101242416 C0	13.08.2008
		CN 1602470 A	30.03.2005
		CN 1602470 C0	09.04.2008
		EP 1364297 A2	26.11.2003
		EP 1461704 A2	29.09.2004
		US 2002-0083175 A1	27.06.2002
		US 2003-0070096 A1	10.04.2003
		US 2003-0110274 A1	12.06.2003
		US 2005-0021740 A1	27.01.2005
		US 2005-0044352 A1	24.02.2005
		US 2006-0050719 A1	09.03.2006
		US 2006-0212572 A1	21.09.2006
		US 6907525 B2	14.06.2005
		US 7171683 B2	30.01.2007
		US 7225270 B2	29.05.2007
		US 7313815 B2	25.12.2007
		US 7707305 B2	27.04.2010
		WO 02-33870 A2	25.04.2002
		WO 02-33870 A3	25.04.2002
		WO 03-050644 A2	19.06.2003
		WO 03-050644 A3	19.06.2003
KR 10-2005-0010896 A	28.01.2005	AU 2003-248653 A1	31.12.2003
		CN 1659822 C0	24.08.2005
		EP 1550259 A1	06.07.2005
		JP 2005-530398 A	06.10.2005
		US 2005-0169282 A1	04.08.2005
		WO 03-107590 A1	24.12.2003

A. 발명이 속하는 기술분류(국제특허분류(IPC)) <i>H04L 12/26(2006.01)i</i>		
B. 조사된 분야 조사된 최소문헌(국제특허분류를 기재) H04L 12/26; G06F 17/00; H04L 12/22; H04L 12/28; H04L 9/32 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: Denial of Service Attack, on the fly packet, load balancing, filtering		
C. 관련 문헌		
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2009-0044177 A (주식회사 다산네트웍스) 2009.05.07 전체 명세서 참조.	1-4
A	KR 10-2004-0074367 A (엘지엔시스(주)) 2004.08.25 전체 명세서 참조.	1-4
A	KR 10-2003-0059204 A (웬월 인코퍼레이티드) 2003.07.07 전체 명세서 참조.	1-4
A	KR 10-2005-0010896 A (톰슨 라이선싱 소시에떼 아노님) 2005.01.28 전체 명세서 참조.	1-4
☐ 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 신구성 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 2010년 07월 27일 (27.07.2010)		국제조사보고서 발송일 2010년 07월 27일 (27.07.2010)
ISA/KR의 명칭 및 우편주소 대한민국 특허청 (302-701) 대전광역시 서구 선사로 139, 정부대전청사 팩스 번호 82-42-472-7140		심사관 성경아 전화번호 82-42-481-8171

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2009-0044177 A	2009.05.07	없음	
KR 10-2004-0074367 A	2004.08.25	없음	
KR 10-2003-0059204 A	2003.07.07	AU 2002-13264 A1 AU 2002-213264 A8 AU 2002-360197 A1 AU 2002-360197 B2 CA 2469885-A1 CN 101242415 A CN 101242415 C0 CN 101242416 A CN 101242416 C0 CN 1602470 A CN 1602470 C0 EP 1364297 A2 EP 1461704 A2 US 2002-0083175 A1 US 2003-0070096 A1 US 2003-0110274 A1 US 2005-0021740 A1 US 2005-0044352 A1 US 2006-0050719 A1 US 2006-0212572 A1 US 6907525 B2 US 7171683 B2 US 7225270 B2 US 7313815 B2 US 7707305 B2 WO 02-33870 A2 WO 02-33870 A3 WO 03-050644 A2 WO 03-050644 A3	2002.04.29 2002.04.29 2003.06.23 2008.08.21 2003.06.19 2008.08.13 2008.08.13 2008.08.13 2008.08.13 2005.03.30 2008.04.09 2003.11.26 2004.09.29 2002.06.27 2003.04.10 2003.06.12 2005.01.27 2005.02.24 2006.03.09 2006.09.21 2005.06.14 2007.01.30 2007.05.29 2007.12.25 2010.04.27 2002.04.25 2002.04.25 2003.06.19 2003.06.19
KR 10-2005-0010896 A	2005.01.28	AU 2003-248653 A1 CN 1659822 C0 EP 1550259 A1 JP 2005-530398 A US 2005-0169282 A1 WO 03-107590 A1	2003.12.31 2005.08.24 2005.07.06 2005.10.06 2005.08.04 2003.12.24