



(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。 Int. Cl. (11) 공개번호 10-2007-0003487
H04L 12/56 (2006.01) (43) 공개일자 2007년01월05일

(21) 출원번호 10-2005-0059501
(22) 출원일자 2005년07월02일
심사청구일자 2005년07월02일

(71) 출원인 충남대학교산학협력단
대전광역시 유성구 궁동 220번지 충남대학교

(72) 발명자 권택근
대전 유성구 신성동 두레아파트 106-902
강석민
대전 서구 도마2동 경남아파트 103동 1301호
송일섭
대전 유성구 봉산동 202-11번지 샘하나마을 401호

(74) 대리인 권오식
박창희

전체 청구항 수 : 총 7 항

(54) 이중 TCAM을 이용한 패킷의 분류방법

(57) 요약

본 발명은 일반적인 규칙을 저장하는 일반 TCAM 테이블과 상기 일반적인 규칙의 반전 형태의 규칙을 저장하는 반전 TCAM 테이블을 이중으로 생성시켜 패킷이 수신될 때 수신된 패킷으로부터 추출된 정보를 일반 TCAM 테이블과 상기 일반 TCAM 테이블과 연계된 반전 TCAM 테이블로부터 검색하는 것을 특징으로 하는 이중 TCAM을 이용한 패킷의 분류방법에 관한 것이다. 본 발명은 패킷 분류 규칙의 표현 형태에 따라 두 개의 TCAM 테이블에 나누어 저장함으로써 TCAM의 필요 크기를 줄이는 장점이 있으며, 그로 인해 하드웨어 패킷 분류 기법에서 고가의 하드웨어인 TCAM을 보다 효율적으로 사용할 수 있는 효과가 있다.

대표도

도 4

특허청구의 범위

청구항 1.

이중 TCAM(Ternary Content Addressable Memory)을 이용한 패킷의 분류방법에 있어서,

a) 일반적인 규칙을 저장하는 일반 TCAM 테이블과 상기 일반적인 규칙의 반전 형태의 규칙을 저장하는 반전 TCAM 테이블을 이중으로 생성시켜 패킷이 수신될 때 수신된 패킷으로부터 추출된 정보를 일반 TCAM 테이블과 상기 일반 TCAM 테이블과 반전 TCAM 테이블로부터 검색하는 것을 특징으로 하는 이중 TCAM을 이용한 패킷의 분류방법.

청구항 2.

제 1 항에 있어서,

패킷 분류를 위해 반전 형태의 표현이 있는 규칙을 반전 형태의 규칙을 복수 개의 TCAM 테이블의 엔트리로 확장하지 않고 일반 TCAM 테이블과는 별도의 반전 TCAM 테이블에 하나의 엔트리로 저장하는 것을 특징으로 하는 이중 TCAM을 이용한 패킷의 분류방법.

청구항 3.

제 2 항에 있어서,

일반 TCAM 테이블은 일치 목록과 추가 검색 여부 결정 기능을 포함하는 연계추가정보와 연계되며, 반전 TCAM 테이블은 일치 목록을 포함하는 연계추가정보와 연계되는 것을 특징으로 하는 TCAM을 이용한 패킷의 분류방법.

청구항 4.

제 3 항에 있어서,

일반 TCAM 테이블로부터 검색하는 단계에서 일반 TCAM 테이블로부터의 검색이 성공하면 검색 결과와 연계추가정보의 일치목록을 바탕으로 추가검색 여부를 판단하여 추가검색 여부가 계속으로 결정되면 추가로 반전 TCAM 테이블을 검색하여 반전 TCAM 테이블로부터 검색이 실패하는 경우에 한하여 상기 일반 TCAM 검색결과로 읽은 일치목록의 규칙에 최종적으로 일치되었다고 판정하는 것을 특징으로 하는 TCAM을 이용한 패킷의 분류방법.

청구항 5.

제 3 항에 있어서,

일반 TCAM 테이블로부터 검색하는 단계에서 일반 TCAM 테이블로부터의 검색에 실패하면 일치하는 규칙을 차지 못함을 판정하고 다음 패킷의 수신 준비를 하는 것을 특징으로 하는 TCAM을 이용한 패킷의 분류방법.

청구항 6.

제 5 항에 있어서,

반전 TCAM 테이블로부터 검색하는 단계에서 반전 TCAM 테이블에서의 검색결과가 성공이면 일치하는 규칙을 찾지 못한 것으로 판정하고 다음 패킷의 수신 준비를 하는 것을 특징으로 하는 TCAM을 이용한 패킷의 분류방법.

청구항 7.

패킷 분류를 위해 반전 형태의 표현이 있는 규칙을 반전 형태의 규칙을 복수 개의 TCAM 테이블의 엔트리로 확장하지 않고 일반 TCAM 테이블과는 별도의 반전 TCAM 테이블에 하나의 엔트리로 저장한 패킷의 분류를 위한 이중 TCAM 테이블.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 TCAM(Ternary Content Addressable Memory)을 사용하여 패킷을 분류할 때, 반전 형태(101)의 패킷 분류 규칙(102~108)을 두 개의 TCAM 테이블을 이용하여 저장함으로써 TCAM을 효율적으로 사용하는 기법에 관한 것이다.

라우터, 방화벽과 같은 네트워크 장비에서는 수신되는 패킷의 헤더 정보 - 프로토콜(110), 송수신 주소(111, 112) 그리고 송수신 포트(113, 114) 등 - 를 기준으로 패킷을 분류하게 된다. 네트워크 장비는 패킷을 분류하고 그 패킷이 포함된 분류에 따라 패킷이 전송되어야 할 다음 네트워크 장비의 경로를 판단하거나, 특정 분류에 속한 패킷에 미리 지정된 서비스 품질을 제공하거나, 현재 패킷을 위험하다고 판단하여 경고하는 등의 다양한 행동(102)을 취할 수 있다. 즉, 네트워크 장비에서 패킷의 정보에 따라 어떠한 행동을 취하려 할 때 우선 패킷을 분류해야만 한다.

네트워크 장비에서 패킷을 분류하는 방법은 크게 소프트웨어를 이용한 방법과 하드웨어를 이용하는 방법으로 나뉜다. TCAM을 이용한 패킷 분류 방법은 후자인 하드웨어를 이용하는 방법으로써 초당 수십억 비트의 패킷을 고속으로 분류하는데 매우 적절한 방법이다.

TCAM은 패킷을 분류하는 규칙을 미리 저장하고, 패킷이 수신되면(202) 그 패킷의 헤더 정보를 추출(203)한 후 TCAM에 저장된 분류 규칙과 일치하는지 한 번의 검색 연산(204)으로 결과를 얻을 수 있는 하드웨어이다.

또한 TCAM은 패킷의 헤더 정보와 TCAM에 저장된 분류 규칙을 비교할 때, 무시 비트 (don't-care bit)를 제공(115, 116)함으로써 유연한 비교 방법을 제공한다. 즉, 특정 열의 무시 비트 표시는 그 열과 일치하는지 검사하는 수신된 패킷의 헤더 정보에 있는 값이 어느 값이든 개의치 않는 것을 의미한다. 이 무시 비트를 이용하여 완전 일치 (exact match), 최장 접두 주소 일치 등의 다양한 일치 방법을 수행할 수 있다.

앞서 언급한 TCAM을 이용한 하드웨어 패킷 분류 방법은 고속 패킷 분류를 위한 기법으로 널리 사용되고 있으며, 특히 한번의 검색 연산으로 일치 결과를 얻을 수 있다는 장점과, 무시 비트를 이용한다는 장점으로 인해 침입 탐지 시스템 (IDS : Intrusion Detection System) 또는 침입 방지 시스템 (IPS : Intrusion Prevention System)에서 널리 사용된다. 이러한 IDS/IPS 시스템은 패킷 분류 정보인 규칙을 미리 정의하고 그 내용을 TCAM에 저장하게 된다. 예를 들어 도 1의 (a)에 침입 탐지 시스템인 Snort의 규칙 예제가 나오는데 그 내용은 tcp 프로토콜(103)이면서 \$EXTERNAL_NET(104)의 어떤 포트(105)로부터 송신되고 \$HOME_NET(107)의 80 포트(108)로 수신되는 패킷이 검출되면 alert(102) 시키라는 규칙이다. 이때 일반적으로 \$EXTERNAL_NET은 \$HOME_NET의 반전으로 미리 정의(101)가 된다. Snort의 2300 여개의 분류 규칙들의 대부분은 이렇게 \$EXTERNAL_NET 변수를 사용하여 반전 형태의 규칙으로 정의가 되어 있다. 이러한 규칙을 TCAM에 저장하고자 할 때, TCAM의 특성상 반전 형태는 TCAM에 직접 한 개의 열로 저장할 수 없다. 그래서 종래의 bit-by-bit flip 표현법에서는 반전 표현할 내용의 bit 값의 역을 구해서 한비트씩 저장하고 나머지 부분을 무시 비트로 채우는 기법(115)을 사용하였다. 도 1에 예로서 나타낸 바와 같이 기재된 도 1 (a)에 예시된 규칙을 bit-by-bit 표현으로 TCAM에 저장할 경우 송신 주소의 반전 표현에 대한 TCAM 내용이 도 1의 (c) 형태로 표현되게 된다. 이처럼 종래의 기술로 반전 형태의 규칙을 TCAM에 저장할 경우 규칙을 확장하여 표현한 후 TCAM에 저장하기 때문에, TCAM의 열의 수가 증가하여 TCAM의 용량을 낭비하게 되는 단점이 있다.

발명이 이루고자 하는 기술적 과제

본 발명은 앞서 언급한 문제점을 극복하기 위하여 안출된 것으로서, 본 발명의 목적은 일반적인 규칙을 저장하는 일반 TCAM 테이블과 상기 일반적인 규칙의 반전 형태의 규칙을 저장하는 반전 TCAM 테이블을 이중으로 d지하여 운영함으로써 요구되는 TCAM의 크기를 효율적으로 줄이는 방법을 제공하는 것을 목적으로 한다.

발명의 구성

본 발명은 이중 TCAM(Ternary Content Addressable Memory)을 이용한 패킷의 분류방법에 있어서, a) 일반적인 규칙을 저장하는 일반 TCAM 테이블과 상기 일반적인 규칙의 반전 형태의 규칙을 저장하는 반전 TCAM 테이블을 이중으로 생성시키는 단계; b) 패킷이 수신될 때 수신된 패킷으로부터 추출된 정보를 일반 TCAM 테이블과 상기 일반 TCAM 테이블과 연계된 반전 TCAM 테이블로부터 검색하는 단계를 특징으로 하며, TCAM 테이블을 패킷 분류를 위해 반전 형태의 표현이 있는 규칙을 반전 형태의 규칙을 복수 개의 TCAM 테이블의 엔트리로 확장하지 않고 일반 TCAM 테이블과는 별도의 반전 TCAM 테이블에 하나의 엔트리로 저장하여 운영하는 것을 특징으로 한다.

상기 일반 TCAM 테이블은 일치 목록과 추가 검색 여부 결정 기능을 포함하는 연계추가정보와 연계되며, 반전 TCAM 테이블은 일치 목록을 포함하는 연계추가정보와 연계되어 구성된다.

상기와 같이 구비된 이중 TCAM 테이블을 바탕으로 패킷이 수신될 때 수신된 패킷으로부터 추출된 정보를 일반 TCAM 테이블과 상기 일반 TCAM 테이블과 연계된 반전 TCAM 테이블로부터 검색하는 단계에서 일반 TCAM 테이블로부터 검색이 성공하면 검색 결과와 연계추가정보의 일치목록을 바탕으로 추가검색 여부를 판단하여 추가검색 여부가 계속으로 결정되면 추가로 반전 TCAM 테이블을 검색하여 반전 TCAM 테이블로부터 검색이 실패하는 경우에 한하여 상기 일반 TCAM 검색결과로 읽은 일치목록의 규칙에 최종적으로 일치되었다고 판정함으로써 수신된 패킷을 분류한다.

이때 일반 TCAM 테이블로부터 검색에 실패하면 일치하는 규칙을 차지 못함을 판정하고 다음 패킷의 수신 준비를 하며, 반전 TCAM 테이블에서 검색결과가 성공이면 일치하는 규칙을 찾지 못한 것으로 판정하고 다음 패킷의 수신 준비한다.

상기한 본 발명의 목적 및 특징들, 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이다. 이하 첨부된 도면을 참조하여 본 발명에 대해 상세히 설명하나, 이러한 설명이 본 발명을 한정하는 것은 아니다.

도 1의 (a)는 널리 쓰이는 IDS 시스템인 Snort의 패킷 분류 규칙(102~108)의 한 예이다. Snort의 규칙 중 하나의 헤더 부분을 도시하였는데 tcp 프로토콜(102)이면서 외부 네트워크(104)의 어떤 포트(105)에서 내부 네트워크(107)의 80 포트(108)로 수신(106)되는 패킷이 검출되면 경고(102)하라는 규칙이다. 일반적으로 Snort에서는 \$EXTERNAL_NET을 \$HOME_NET으로 정의(101)하기 때문에 수많은 Snort 규칙에 반전 형태의 규칙이 존재하게 된다.

도 1의 (b)는 \$HOME_NET이 10.0.0.0/24 네트워크라고 가정할 때(109) 도 1의 (a)의 규칙에 검출되는 패킷의 예(110~114)를 도시하였다. 송신 포트의 경우 규칙에 any(105)로 표현되었기 때문에 실제 패킷의 송신 포트(113)는 비교할 필요가 없다.

도 1의 (c)는 기존의 bit-by-bit flip 표현법을 이용하였을 경우, 일정한 가정(116) 하에 도 1의 (a)의 규칙을 TCAM에 저장하면 규칙이 확장되어 TCAM의 열의 수가 증가하는 예를 도시하였다. 만약 \$HOME_NET이 10.0.0.0/24 라고 가정하면 규칙 하나에 대해 TCAM의 열의 수는 24개로 증가하게 되는 문제가 있다. 최악의 경우 - 10.0.0.0/32 같은 - TCAM의 열의 수는 한 개의 규칙으로 인해 32개로 증가한다.

도 2는 일반적으로 TCAM을 사용하여 패킷을 분류하는 네트워크 장비에서의 순서도를 도시하였다. 패킷이 수신(202)되면 그 패킷에서 5-튜플 정보(프로토콜, 송수신 주소 그리고 송수신 포트)를 추출(203)하고 이 정보를 이용하여 미리 규칙을 저장한 TCAM에 5-튜플 정보가 일치하는 규칙이 있는지 검색(204)한다. 검색 결과가 없다면 그대로 패킷을 송신(206)하고, 검색 결과가 있다면 검색 결과(TCAM의 특정 열)에 연계된 추가 정보를 읽어온 후(207) 그 정보의 내용에 따라 특정 행동 - 경고, 패킷 폐기 등 - 을 취하게 된다(208)

도 3은 규칙 확장의 문제를 해결하기 위해 본 발명에서 제안하는 이중 TCAM 테이블을 이용하여 규칙을 저장하는 예를 도시한 것이다. 본 발명에서는 TCAM에 두 개의 테이블을 유지한다. 하나는 일반 TCAM 테이블(305)이고 다른 하나는 반전 TCAM 테이블(312)이다. 도 3의 (a)에 예제 분류 규칙을 2개(301) 도시한 것이다. 이때 참고의 내용(304)을 가정한다. 이 두 개의 규칙 중 규칙 1은 반전 형태의 표현이 없고 규칙 2는 송신 주소(302), 수신 주소(303) 부분에 반전 형태의 표현이 존재한다. 이 규칙 2개는 도 3의 (b)의 내용대로 TCAM에 저장된다. 우선 일반 테이블에는 규칙 1의 내용이 저장된다. 그

리고 이 열과 연계된 정보의 일치 목록에 규칙 1이 저장된 열이라는 표시(306)를 하고 추가 검색 여부에 중지라고 표시(307)를 한다. 규칙 1은 반전 형태가 없으므로 반전 테이블에는 저장하지 않는다. 이제 규칙 2를 저장하는데, 송신 주소, 수신 주소 모두 반전 형태이므로 이런 경우는 일반 TCAM 테이블에 모두 무시 비트를 이용한 열(308, 309)을 저장하고 연계추가정보에 규칙 2의 열이라는 표시(310)와 추가 검색을 계속하라는 표시(311)도 저장한다. 또한 규칙 2를 반전 테이블에 저장하는데, 반전 표시가 있는 행의 수와 동일한 수의 반전 테이블의 열로 저장하는데 이때 반전 표시를 제외하고 저장한다. 예에서는 2개의 열이 저장된다. 송신 주소(313)를 기준으로 저장할 때는 수신 주소 부분은 무시 비트로 저장(314)하고 일치 목록에 규칙 2라고 표시한다. 수신 주소(316)를 기준으로 저장할 때는 송신 주소 부분은 무시 비트로 저장(315)하고 일치 목록에 규칙 2라고 표시한다. 도 3의 (c)에는 (a), (b)의 내용에 따라 시스템이 구성된 경우 실제 패킷에 따른 검색 결과의 예를 보여준다. 패킷 1은 일반 테이블의 검색에 성공(317)하고 더 이상 검색을 하지 않으므로(319) 최종적으로 일치 목록(318)에 따라 규칙 1에 일치한다고 결과가 판명(321)된다. 패킷 2는 일반 테이블의 검색에 성공(322)하고 추가 검색이 계속(324)이므로 반전 테이블을 검색한 후 검색에 실패(325)하므로 일치 목록(323)에 따라 규칙 2에 일치한다고 결과가 판명(326)된다. 패킷 3은 일반 테이블의 검색에 성공(327)하고, 반전 테이블의 검색에도 성공(33)하였기 때문에 최종적으로 일치 정보를 발견하지 못했다고 판명(331)된다.

도 4는 이중 TCAM 테이블을 이용하여 수신된 패킷이 일치하는 규칙을 찾는 순서도를 도시한 것이다. 앞서 언급한 대로 패킷이 수신되면 5-튜플 정보를 추출(401)한다. 그리고 일반 테이블을 검색(402)한다. 검색에 실패하면 일치하는 규칙을 찾지 못함으로 판명(409)하고 다음 패킷의 수신을 준비(401)한다. 검색에 성공하면, 검색 결과의 연계추가정보를 읽어 일치 목록과 추가 검색 여부(404)를 알아낸다. 추가 검색 여부가 중지이면 현재 일치된 규칙을 최종 결과로 판정(406)하고 다시 패킷 수신을 준비(401)한다. 추가 검색 여부가 계속이면 이번에는 반전 테이블을 검색(407)한다. 반전 테이블 검색 결과가 실패이면, 일반 테이블 검색 결과로 읽은 일치 목록의 규칙에 최종적으로 일치되었다고 판정(406)하고 다시 패킷 수신 과정(401)으로 돌아간다. 반전 테이블 검색 결과가 성공이면, 일치되는 규칙을 찾지 못했다고 판정(408)하고 패킷 수신 과정(401)으로 돌아간다.

상기 설명에서 알 수 있듯이 일반 테이블에 검색이 성공하면 일치하는 규칙이 있을 가능성이 있는 것으로 판정을 하고, 추가 검색 여부에 따라 최종 결과를 판정 한다. 또한 반전 테이블에 검색이 성공하면 일치하는 규칙이 없다고 판정을 한다. 그 이유는 패킷 분류 규칙을 TCAM 테이블에 저장할 때, 일치해야 하는 규칙은 일반 테이블에, 일치하지 않아야 하는 - 즉, 반전 형태로 표현된 - 규칙은 반전 테이블에 저장하기 때문에, 이러한 판정 과정을 거친다. 이렇게 두 개의 TCAM 테이블을 사용하지만 반전 형태의 규칙을 확장할 필요 없이 그대로 저장하여 고가의 하드웨어인 TCAM을 보다 효율적으로 사용할 수 있는 장점이 있다.

발명의 효과

이상에서 상세히 설명한 바와 같이 본 발명은, TCAM을 이용한 패킷 분류 기법에서, 패킷 분류 규칙의 표현 형태에 따라 두 개의 TCAM 테이블에 나누어 저장함으로써 TCAM의 필요 크기를 줄이는 효과가 있으며, 그로 인해 하드웨어 패킷 분류 기법에서 고가의 하드웨어인 TCAM을 보다 효율적으로 사용할 수 있는 장점이 있다.

도면의 간단한 설명

도 1은 본 발명에 적용되는 패킷 분류 규칙인 Snort의 예와 패킷의 예, 그리고 이러한 규칙을 TCAM에 저장하는 종래의 기법인 bit-by-bit flip 표현도이고,

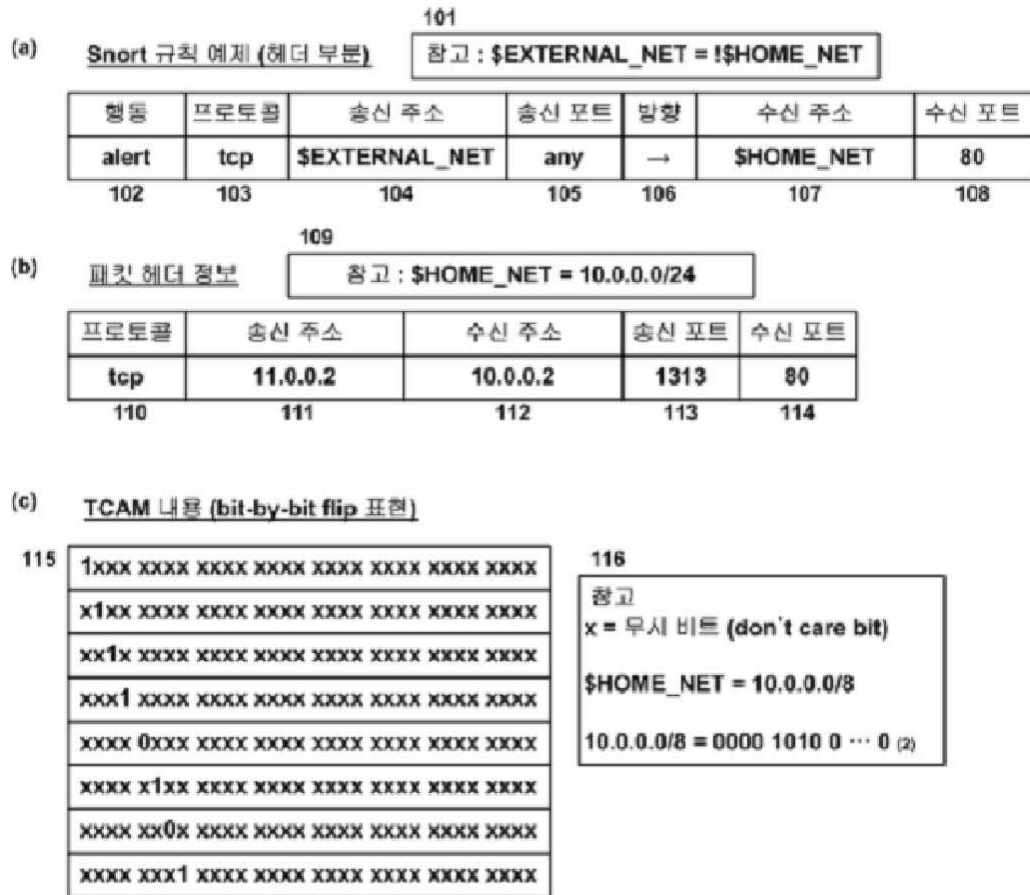
도 2는 본 발명에 적용되는 TCAM을 이용한 패킷 분류 시스템의 흐름도이며,

도 3은 본 발명에 따른 이중 TCAM 테이블을 이용하여 예제 규칙을 적용한 TCAM의 내용, 그리고 규칙의 적용 예이고,

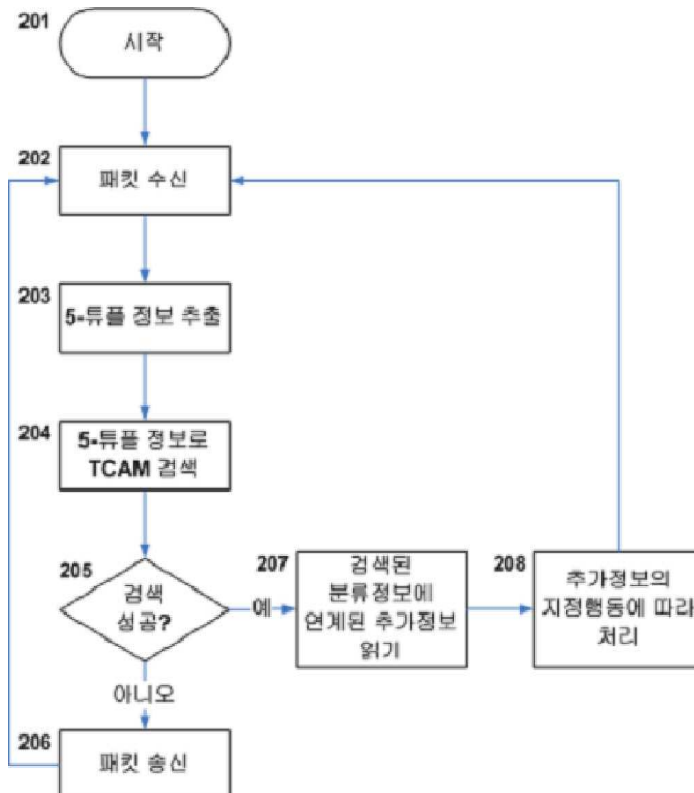
도 4는 본 발명에 따른 패킷이 해당하는 규칙이 이중 TCAM 테이블에 존재하는지 여부를 판정하는 흐름도이다.

도면

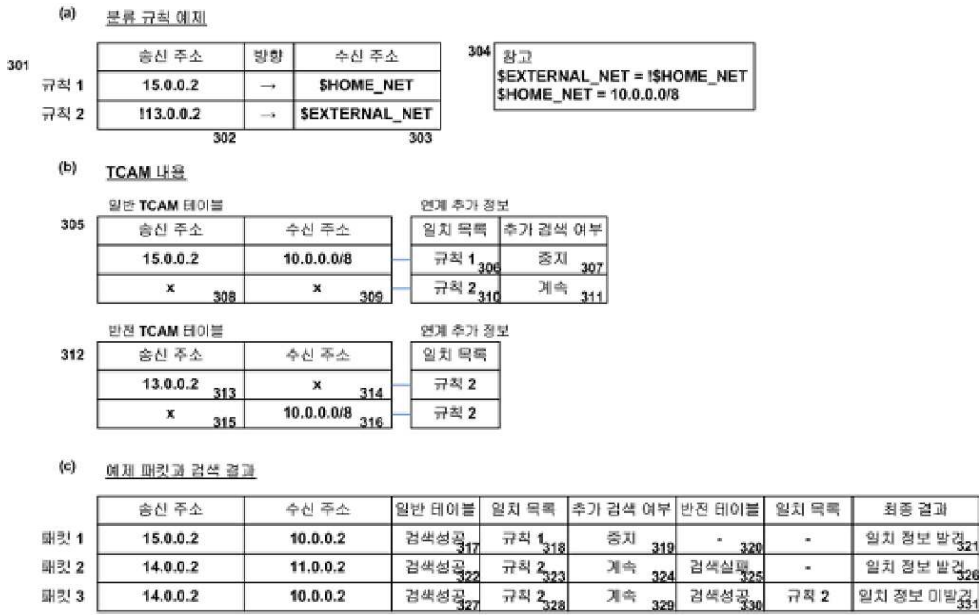
도면1



도면2



도면3



도면4

