(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년06월09일
(11) 등록번호 10-1527149
(24) 등록일자 2015년06월02일

(51) 국제특허분류(Int. Cl.)
H04L 12/26 (2006.01) *H04L 12/70* (2013.01)
(21) 출원번호 10-2014-0036310
(22) 출원일자 2014년03월27일
심사청구일자 2014년03월27일
(56) 선행기술조사문헌
KR101284584 B1
KR1020060096077 A

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
김명섭
세종특별자치시 조치원읍 도원1로 16, 111-902 (푸르지오1차)
이수강
서울특별시 마포구 월드컵북로 501, 914동302호 (상암동, 상암월드컵파크9단지)
안현민
제주특별자치도 제주시 구남로2길 36 , 401호 (이도이동)
(74) 대리인
심경식, 홍성욱, 한승범, 유병욱

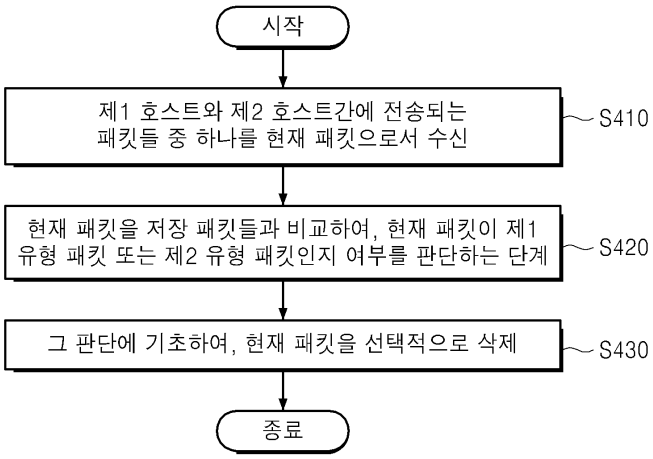
전체 청구항 수 : 총 8 항 심사관 : 전용해

(54) 발명의 명칭 **중복 패킷을 방지하는 패킷 처리 방법 및 그 장치**

(57) 요 약

중복 패킷을 방지하는 패킷 처리 방법이 개시된다. 본 발명의 일 실시예에 따른 패킷 처리 방법은 제1 호스트와 제2 호스트간에 전송되는 패킷들 중 하나를 현재 패킷으로서 수신하는 단계; 상기 현재 패킷을 상기 현재 패킷 이전에 수신되어 저장된 저장 패킷들과 비교하여, 상기 현재 패킷이 상기 저장 패킷들 중 하나와 동일한 페이로드 값을 포함하는 제1 유형 패킷 또는 상기 제1 유형 패킷과 관련된 패킷으로서 상기 제1 유형 패킷 이후에 수신된 제2 유형 패킷인지 여부를 판단하는 단계; 및 상기 판단에 기초하여, 상기 현재 패킷을 선택적으로 삭제하는 단계를 포함한다.

대 표 도 - 도4



명 세 서

청구범위

청구항 1

중복 패킷을 방지하는 패킷 처리 방법에 있어서,

제1 호스트와 제2 호스트간에 전송되는 패킷들 중 하나를 현재 패킷으로서 수신하는 단계;

상기 현재 패킷을 상기 현재 패킷 이전에 수신되어 저장된 저장 패킷들과 비교하여, 상기 현재 패킷이 상기 저장 패킷들 중 하나와 동일한 페이로드 값을 포함하는 제1 유형 패킷 또는 상기 제1 유형 패킷과 관련된 패킷으로서 상기 제1 유형 패킷 이후에 수신된 제2 유형 패킷인지 여부를 판단하는 단계; 및

상기 판단에 기초하여, 상기 현재 패킷을 선택적으로 삭제하는 단계를 포함하고,

상기 판단하는 단계는 상기 현재 패킷의 전송 방향과 동일한 전송 방향의 저장 패킷들 중에서 가장 큰 시퀀스 번호를 가진 저장 패킷인 기준 패킷의 시퀀스 번호와 패킷 길이 값을 합산한 합산 값이 상기 현재 패킷의 시퀀스 번호보다 작으면 상기 현재 패킷을 상기 제2 유형 패킷으로 판단하고,

상기 현재 패킷을 선택적으로 삭제하는 단계는 상기 제2 유형 패킷으로 판단된 상기 현재 패킷을 삭제하고,

상기 제1유형 패킷은 상기 저장 패킷들 중 하나와 동일한 페이로드 값, 동일한 시퀀스 번호 및 동일한 패킷 길이 값을 가지는 일반적인 중복 패킷과 상기 저장 패킷들 중 하나와 동일한 페이로드 값, 동일한 시퀀스 번호 및 상이한 패킷 길이 값을 가지는 재패킷화된 중복 패킷을 포함하고,

상기 제2유형 패킷은 상기 재패킷화된 중복 패킷과 관련된 패킷으로서 상기 재패킷화된 중복 패킷 이후에 수신된 패킷이고, 상기 제2유형 패킷의 시퀀스 번호는 상기 저장 패킷들의 시퀀스 번호와 상이한 것을 특징으로 하는 패킷 처리 방법.

청구항 2

제1항에 있어서,

상기 판단하는 단계는

상기 현재 패킷 및 상기 저장 패킷들의 시퀀스 번호, 전송 방향, ACK 번호 및 패킷 길이 값 중 적어도 하나에 기초하여 수행되는 것을 특징으로 하는 패킷 처리 방법.

청구항 3

제1항에 있어서,

상기 판단하는 단계는 상기 저장 패킷들 중에서 상기 현재 패킷의 전송 방향과 동일한 전송 방향을 가지고 상기 현재 패킷의 시퀀스 번호와 동일한 시퀀스 번호를 가지는 저장 패킷이 존재하면 상기 현재 패킷을 상기 제1 유형 패킷으로 판단하고,

상기 현재 패킷을 선택적으로 삭제하는 단계는 상기 제1 유형 패킷으로 판단된 상기 현재 패킷을 삭제하는 것을 특징으로 하는 패킷 처리 방법.

청구항 4

삭제

청구항 5

제1항에 있어서,

상기 판단하는 단계는

상기 현재 패킷의 전송 방향과 동일한 전송 방향의 저장 패킷들 중에서 가장 큰 시퀀스 번호를 가진 저장 패킷

인 기준 패킷을 검출하는 단계;

상기 기준 패킷과 상기 현재 패킷의 시퀀스 번호 및 패킷 길이 값을 이용하여 상기 패킷들을 비교하는 단계; 및

상기 비교 결과에 기초하여, 상기 현재 패킷이 상기 제1 유형 패킷 또는 상기 제2 유형 패킷인지 여부를 판단하는 단계를 포함하는 것을 특징으로 하는 패킷 처리 방법.

청구항 6

트래픽 수집 지점에서의 중복 패킷을 방지하는 패킷 처리 장치에 있어서,

제1 호스트와 제2 호스트간에 전송되는 패킷들 중 하나를 현재 패킷으로서 수신하는 수신부;

상기 현재 패킷을 상기 현재 패킷 이전에 수신되어 저장된 저장 패킷들과 비교하여, 상기 현재 패킷이 상기 저장 패킷들 중 하나와 동일한 페이로드 값을 포함하는 제1 유형 패킷 또는 상기 제1 유형 패킷과 관련된 패킷으로서 상기 제1 유형 패킷 이후에 수신된 제2 유형 패킷인지 여부를 판단하는 판단부; 및

상기 판단에 기초하여, 상기 현재 패킷을 선택적으로 삭제하는 패킷 처리부를 포함하고,

상기 판단부는 상기 현재 패킷의 전송 방향과 동일한 전송 방향의 저장 패킷들 중에서 가장 큰 시퀀스 번호를 가진 저장 패킷인 기준 패킷의 시퀀스 번호와 패킷 길이 값을 합산한 합산 값이 상기 현재 패킷의 시퀀스 번호보다 작으면 상기 현재 패킷을 상기 제2 유형 패킷으로 판단하고,

상기 패킷 처리부는 상기 제2 유형 패킷으로 판단된 상기 현재 패킷을 삭제하고,

상기 제1유형 패킷은 상기 저장 패킷들 중 하나와 동일한 페이로드 값, 동일한 시퀀스 번호 및 동일한 패킷 길이 값을 가지는 일반적인 중복 패킷과 상기 저장 패킷들 중 하나와 동일한 페이로드 값, 동일한 시퀀스 번호 및 상이한 패킷 길이 값을 가지는 재패킷화된 중복 패킷을 포함하고,

상기 제2유형 패킷은 상기 재패킷화된 중복 패킷과 관련된 패킷으로서 상기 재패킷화된 중복 패킷 이후에 수신된 패킷이고, 상기 제2유형 패킷의 시퀀스 번호는 상기 저장 패킷들의 시퀀스 번호와 상이한 것을 특징으로 하는 패킷 처리 장치.

청구항 7

제6항에 있어서,

상기 판단부는

상기 현재 패킷 및 상기 저장 패킷들의 시퀀스 번호, 전송 방향, ACK 번호 및 패킷 길이 값 중 적어도 하나에 기초하여 상기 판단을 수행하는 것을 특징으로 하는 패킷 처리 장치.

청구항 8

제6항에 있어서,

상기 판단부는 상기 저장 패킷들 중에서 상기 현재 패킷의 전송 방향과 동일한 전송 방향을 가지고 상기 현재 패킷의 시퀀스 번호와 동일한 시퀀스 번호를 가지는 저장 패킷이 존재하면 상기 현재 패킷을 상기 제1 유형 패킷으로 판단하고,

상기 패킷 처리부는 상기 제1 유형 패킷으로 판단된 상기 현재 패킷을 삭제하는 것을 특징으로 하는 패킷 처리 장치.

청구항 9

삭제

청구항 10

제6항에 있어서,

상기 판단부는

상기 현재 패킷의 전송 방향과 동일한 전송 방향의 저장 패킷들 중에서 가장 큰 시퀀스 번호를 가진 저장 패킷

인 기준 패킷을 검출하는 패킷 검출부;

상기 기준 패킷과 상기 현재 패킷의 시퀀스 번호 및 패킷 길이 값을 이용하여 상기 패킷들을 비교하는 비교부; 및

상기 비교 결과에 기초하여, 상기 현재 패킷이 상기 제1 유형 패킷 또는 상기 제2 유형 패킷인지 여부를 판단하는 패킷 판단부를 포함하는 것을 특징으로 하는 패킷 처리 장치.

청구항 11

삭제

청구항 12

삭제

발명의 설명

기 술 분 야

[0001] 본 발명의 일 실시예는 패킷 처리에 관한 것으로, 특히 중복 패킷 발생을 방지하는 패킷 처리 방법 및 그 장치에 관한 것이다.

배 경 기 술

[0002] 초고속 인터넷의 보급과 다양한 인터넷 기반 응용(application)의 등장으로 인해 트래픽이 복잡 다양해지고 있다. 이러한 상황 속에서 효과적인 네트워크의 관리를 위해 패킷을 발생시킨 응용을 탐지할 수 있어야 한다.

[0003] 트래픽 분석을 위한 응용을 탐지하는 방법으로는 대표적으로 통계정보 트래픽 분류 방법이 사용되는데, 이 방법에서는 패킷의 크기와 전송 방향, 전송 순서, 캡쳐 시간 등을 사용하여 트래픽을 분류한다. 하지만, 수집된 통계정보를 그대로 사용하여 트래픽을 분류하게 되면 문제가 발생할 수 있는데, 중복 패킷이 발생할 수 있기 때문이다. 중복 패킷이 발생하는 상황에 대해서는 이하에서 도 1을 참조하여 설명한다.

[0004] 도 1은 중복 패킷 발생 상황을 설명하기 위하여 도시한 도면이다.

[0005] 도 1을 참조하면, 호스트 A가 호스트 B에게 a-b-e-f-g의 순서로 패킷을 전송하는 중에 g 패킷은 호스트 B에 전달되지 않게되는데, 이에 따라 호스트 A는 g 패킷과 동일한 패킷인 h 패킷을 재전송 패킷으로서 호스트 B에게 전송하게 된다. 이때, 트래픽 수집 지점 C1과 C2에는 g 패킷과 h 패킷이 모두 수신되는데, g 패킷과 h 패킷은 동일한 패킷이므로 중복 패킷이 발생하게 된다.

[0006] 한편, 도 1에서 호스트 A는 h 패킷을 전송한 후에 일정 시간이 흘렀음에도 h 패킷에 대한 응답 패킷을 수신하지 못하여 재패킷화된 재전송 패킷인 i 패킷을 호스트 B에게 전송하게 된다. 이때, 재패킷화된 재전송 패킷이란 원래의 패킷과 시퀀스 번호는 같으나 패킷의 크기가 다른 패킷을 말하는데, 성능 향상을 목적으로 패킷의 최대 크기 범위 내에서 원래 패킷에 포함되었던 페이로드 값에 추가적인 페이로드 값을 삽입함으로써 생성된다.

[0007] 이와 같이, 호스트 A가 재패킷화된 재전송 패킷인 i 패킷을 호스트 B에게 전송하면 호스트 B는 그에 대한 응답 패킷인 k 패킷을 호스트 A에게 전송하게 된다. 또한, 호스트 A는 응답 패킷 k를 수신하면 재패킷화된 재전송 패킷인 i 패킷에 이어진 시퀀스 번호를 가진 m 패킷을 생성하여 호스트 B에게 전송하게 된다.

[0008] 이때, 트래픽 수집 지점 C1과 C2에는 g 패킷, h 패킷이 저장되어 있는데, 재패킷화된 재전송 패킷인 i 패킷에 포함된 페이로드 값이 g 패킷 및 h 패킷의 페이로드 값과 겹치게 되므로 g 패킷, h 패킷 및 i 패킷은 중복 패킷이 된다.

[0009] 이와 같이, 트래픽 수집 지점들에서 중복 패킷이 발생하게 되면, 그 중복 패킷이 발생한 트래픽 수집 지점들에서의 트래픽 분석 결과에 오류가 발생하게 되어 트래픽 분석 결과를 신뢰할 수 없게 된다.

[0010] 따라서, 신뢰성 있는 트랙픽 분석 결과를 보장하기 위해 트래픽 수집 지점에서의 중복 패킷 발생을 방지하기 위한 방안의 필요성이 대두되고 있다.

발명의 내용

해결하려는 과제

[0011] 본 발명의 일 실시예의 목적은 중복 패킷 발생을 방지함으로써 트래픽 분석 결과의 신뢰도를 향상시킬 수 있는 패킷 처리 방법 및 그 장치를 제공하는 것이다.

과제의 해결 수단

[0012] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 중복 패킷을 방지하는 패킷 처리 방법은 제1 호스트와 제2 호스트간에 전송되는 패킷들 중 하나를 현재 패킷으로서 수신하는 단계; 상기 현재 패킷을 상기 현재 패킷 이전에 수신되어 저장된 저장 패킷들과 비교하여, 상기 현재 패킷이 상기 저장 패킷들 중 하나와 동일한 페이로드 값을 포함하는 제1 유형 패킷 또는 상기 제1 유형 패킷과 관련된 패킷으로서 상기 제1 유형 패킷 이후에 수신된 제2 유형 패킷인지 여부를 판단하는 단계; 및 상기 판단에 기초하여, 상기 현재 패킷을 선택적으로 삭제하는 단계를 포함한다.

[0013] 바람직하게는, 상기 판단하는 단계는 상기 현재 패킷 및 상기 저장 패킷들의 시퀀스 번호, 전송 방향, ACK 번호 및 패킷 길이 값 중 적어도 하나에 기초하여 수행될 수 있다.

[0014] 바람직하게는, 상기 판단하는 단계는 상기 저장 패킷들 중에서 상기 현재 패킷의 전송 방향과 동일한 전송 방향을 가지고 상기 현재 패킷의 시퀀스 번호와 동일한 시퀀스 번호를 가지는 저장 패킷이 존재하면 상기 현재 패킷을 상기 제1 유형 패킷으로 판단하고, 상기 현재 패킷을 선택적으로 삭제하는 단계는 상기 제1 유형 패킷으로 판단된 상기 현재 패킷을 삭제할 수 있다.

[0015] 바람직하게는, 상기 판단하는 단계는 상기 현재 패킷의 전송 방향과 동일한 전송 방향의 저장 패킷들 중에서 가장 큰 시퀀스 번호를 가진 저장 패킷인 기준 패킷의 시퀀스 번호와 패킷 길이 값을 합산한 합산 값이 상기 현재 패킷의 시퀀스 번호보다 작으면 상기 현재 패킷을 상기 제2 유형 패킷으로 판단하고, 상기 현재 패킷을 선택적으로 삭제하는 단계는 상기 제2 유형 패킷으로 판단된 상기 현재 패킷을 삭제할 수 있다.

[0016] 바람직하게는, 상기 판단하는 단계는 상기 현재 패킷의 전송 방향과 동일한 전송 방향의 저장 패킷들 중에서 가장 큰 시퀀스 번호를 가진 저장 패킷인 기준 패킷을 검출하는 단계; 상기 기준 패킷과 상기 현재 패킷의 시퀀스 번호 및 패킷 길이 값을 이용하여 상기 패킷들을 비교하는 단계; 및 상기 비교 결과에 기초하여, 상기 현재 패킷이 상기 제1 유형 패킷 또는 상기 제2 유형 패킷인지 여부를 판단하는 단계를 포함할 수 있다.

[0017] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 트래픽 수집 지점에서의 중복 패킷을 방지하는 패킷 처리 장치는 제1 호스트와 제2 호스트간에 전송되는 패킷들 중 하나를 현재 패킷으로서 수신하는 수신부; 상기 현재 패킷을 상기 현재 패킷 이전에 수신되어 저장된 저장 패킷들과 비교하여, 상기 현재 패킷이 상기 저장 패킷들 중 하나와 동일한 페이로드 값을 포함하는 제1 유형 패킷 또는 상기 제1 유형 패킷과 관련된 패킷으로서 상기 제1 유형 패킷 이후에 수신된 제2 유형 패킷인지 여부를 판단하는 판단부; 및 상기 판단에 기초하여, 상기 현재 패킷을 선택적으로 삭제하는 패킷 처리부를 포함한다.

[0018] 바람직하게는, 상기 판단부는 상기 현재 패킷 및 상기 저장 패킷들의 시퀀스 번호, 전송 방향, ACK 번호 및 패킷 길이 값 중 적어도 하나에 기초하여 상기 판단을 수행할 수 있다.

[0019] 바람직하게는, 상기 판단부는 상기 저장 패킷들 중에서 상기 현재 패킷의 전송 방향과 동일한 전송 방향을 가지고 상기 현재 패킷의 시퀀스 번호와 동일한 시퀀스 번호를 가지는 저장 패킷이 존재하면 상기 현재 패킷을 상기 제1 유형 패킷으로 판단하고, 상기 패킷 처리부는 상기 제1 유형 패킷으로 판단된 상기 현재 패킷을 삭제할 수 있다.

[0020] 바람직하게는, 상기 판단부는 상기 현재 패킷의 전송 방향과 동일한 전송 방향의 저장 패킷들 중에서 가장 큰 시퀀스 번호를 가진 저장 패킷인 기준 패킷의 시퀀스 번호와 패킷 길이 값을 합산한 합산 값이 상기 현재 패킷의 시퀀스 번호보다 작으면 상기 현재 패킷을 상기 제2 유형 패킷으로 판단하고, 상기 패킷 처리부는 상기 제2 유형 패킷으로 판단된 상기 현재 패킷을 삭제할 수 있다.

[0021] 바람직하게는, 상기 판단부는 상기 현재 패킷의 전송 방향과 동일한 전송 방향의 저장 패킷들 중에서 가장 큰 시퀀스 번호를 가진 저장 패킷인 기준 패킷을 검출하는 패킷 검출부; 상기 기준 패킷과 상기 현재 패킷의 시퀀스 번호 및 패킷 길이 값을 이용하여 상기 패킷들을 비교하는 비교부; 및 상기 비교 결과에 기초하여, 상기 현재 패킷이 상기 제1 유형 패킷 또는 상기 제2 유형 패킷인지 여부를 판단하는 패킷 판단부를 포함할 수 있다.

발명의 효과

[0022] 본 발명의 일 실시예에 따르면 중복 패킷의 발생을 방지함으로써 트래픽 분석에 있어서의 트래픽의 미탐지 및 오탐지 가능성을 최소화할 수 있고, 이에 따라 트래픽 분석 결과의 신뢰도를 향상시킬 수 있는 효과가 있다.

도면의 간단한 설명

[0023] 도 1은 중복 패킷 발생 상황을 설명하기 위하여 도시한 도면이다.

도 2는 본 발명의 일 실시예에 따른 중복 패킷 발생을 방지하는 패킷 처리 장치를 설명하기 위하여 도시한 도면이다.

도 3은 본 발명의 일 실시예에 따른 판단부를 설명하기 위하여 도시한 도면이다.

도 4는 본 발명의 일 실시예에 따른 중복 패킷 발생을 방지하는 패킷 처리 방법을 설명하기 위하여 도시한 흐름도이다.

도 5는 본 발명의 일 실시예에 따른 패킷 유형 판단 방법을 설명하기 위하여 도시한 흐름도이다.

도 6은 본 발명의 일 실시예에 따른 중복 패킷 발생을 방지하는 패킷 처리 방법에 대한 의사코드를 나타내는 도면이다.

도 7은 본 발명의 일 실시예에 따른 중복 패킷 발생을 방지하는 패킷 처리 방법을 도 1의 트래픽 수집 지점 C2에 적용하여 설명하기 위하여 도시한 도면이다.

도 8은 본 발명의 일 실시예에 따른 중복 패킷 발생을 방지하는 패킷 처리 장치를 이용한 트래픽 분석 시스템을 설명하기 위하여 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0024] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0025] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0026] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0027] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0028] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0029] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0030] 도 2는 본 발명의 일 실시예에 따른 중복 패킷 발생을 방지하는 패킷 처리 장치를 설명하기 위하여 도시한 도면이다.

[0031] 도 2를 참조하면, 본 발명의 일 실시예에 따른 패킷 처리 장치(200)는 수신부(210), 판단부(220) 및 패킷 처리부(230)를 포함한다. 이때, 패킷 처리 장치(200)는 트래픽 수집 지점에 설치된다고 가정한다.

[0032] 수신부(210)는 제1 호스트(미도시)와 제2 호스트(미도시)간에 전송되는 패킷들 중 하나를 현재 패킷으로서 수신한다.

[0033] 판단부(220)는 수신부(210)를 통해 수신된 현재 패킷을 현재 패킷 이전에 수신되어 패킷 처리 장치(200)에 저장된 저장 패킷들과 비교하여, 현재 패킷이 저장 패킷들 중 하나와 동일한 페이로드 값을 포함하는 제1 유형 패킷 또는 제1 유형 패킷과 관련된 패킷으로서 제1 유형 패킷 이후에 수신된 제2 유형 패킷인지 여부를 판단한다.

[0034] 이때, 판단부(220)는 현재 패킷 및 저장 패킷들의 시퀀스 번호, 전송 방향, ACK 번호, 패킷 길이 값 등에 기초하여 동작을 수행할 수 있다.

[0035] 또한, 판단부(220)는 저장 패킷들 중에서 현재 패킷의 전송 방향과 동일한 전송 방향을 가지고 현재 패킷의 시퀀스 번호와 동일한 시퀀스 번호를 가지는 저장 패킷이 존재하면 그 현재 패킷을 제1 유형 패킷으로 판단할 수 있다.

[0036] 이때, 제1 유형 패킷은 일반적인 중복 패킷과 재패킷화된 중복 패킷을 모두 포함하는 개념으로, 일반적인 중복 패킷은 현재 패킷이 동일한 전송방향을 가지는 저장 패킷들 중 하나와 동일한 페이로드 값과 동일한 패킷 길이 값을 가지는 경우이고, 재패킷화된 중복 패킷은 현재 패킷이 동일한 전송 방향을 가지는 저장 패킷들 중 하나와 동일한 페이로드 값을 갖지만 추가적인 페이로드 값을 더 가져 더 큰 패킷 길이 값을 가지는 경우이다.

[0037] 다른 실시예에서는, 판단부(220)가 현재 패킷과 저장 패킷들의 시퀀스 번호, 전송방향, 패킷 길이 값에 기초하여 현재 패킷이 제1 유형 패킷 중에서 일반적인 중복 패킷에 해당하는지 또는 재패킷화된 중복 패킷에 해당하는지 여부를 더 판단할 수 있다.

[0038] 예컨대, 현재 패킷과 저장 패킷들을 비교한 결과, 저장 패킷들 중에 현재 패킷과 동일한 시퀀스 번호, 동일한 전송 방향, 동일한 패킷 길이 값을 가지는 저장 패킷이 존재하면 판단부(220)는 그 현재 패킷을 일반적인 중복 패킷으로 판단할 수 있고, 저장 패킷들 중에 현재 패킷과 동일한 시퀀스 번호, 동일한 전송 방향을 가지면서 현재 패킷의 패킷 길이 값보다 더 큰 패킷 길이 값을 가지는 저장 패킷이 존재하면 판단부(220)는 그 현재 패킷을 재패킷화된 중복 패킷으로 판단할 수 있다.

[0039] 또한, 판단부(220)는 현재 패킷의 전송 방향과 동일한 전송 방향의 저장 패킷들 중에서 가장 큰 시퀀스 번호를 가진 저장 패킷인 기준 패킷의 시퀀스 번호와 패킷 길이 값을 합산한 합산 값이 현재 패킷의 시퀀스 번호보다 작으면 현재 패킷을 제2 유형 패킷으로 판단할 수 있다.

[0040] 판단부(220)의 구체적인 구성에 대해서는 도 3을 참조하여 후술한다.

[0041] 패킷 처리부(230)는 판단부(220)의 판단에 기초하여, 현재 패킷을 선택적으로 삭제한다.

[0042] 보다 구체적으로는, 패킷 처리부(230)는 현재 패킷이 제1 유형 패킷 또는 제2 유형 패킷으로 판단되면 현재 패킷을 삭제하고, 그 외의 경우에는 현재 패킷을 저장한다.

[0043] 종래에는 중복 패킷이 발생하는 경우에 먼저 수신된 패킷을 삭제하였으나, 본 발명의 일 실시예는 미리 수신되어 저장된 저장 패킷과 재전송을 통해 나중에 수신된 현재 패킷이 중복 패킷(제1 유형 패킷)이라고 판단되면, 나중에 수신된 현재 패킷을 삭제함으로써 재전송된 패킷 대신에 최초에 전송한 원래 패킷을 이용하여 트래픽 분석을 할 수 있게 되어 보다 정확한 트래픽 분석을 수행할 수 있게 된다.

[0044] 또한, 본 발명의 일 실시예는 중복 패킷 또는 재패킷화된 중복 패킷을 포함하는 제1 유형 패킷 뿐만 아니라, 제1 유형과 관련된 제2 유형 패킷까지 삭제하기 때문에 중복 패킷으로 인해 발생하는 트래픽 분석 결과의 오류를 최소화할 수 있게 된다.

[0045] 도 3은 본 발명의 일 실시예에 따른 판단부를 설명하기 위하여 도시한 도면이다.

[0046] 도 3을 참조하면, 본 발명의 일 실시예에 따른 판단부(220)는 패킷 검출부(222), 비교부(224) 및 패킷 판단부(226)를 포함한다.

[0047] 패킷 검출부(222)는 현재 패킷의 전송 방향과 동일한 전송 방향의 저장 패킷들 중에서 가장 큰 시퀀스 번호를 가진 저장 패킷인 기준 패킷을 검출한다.

[0048] 이때, 가장 큰 시퀀스 번호를 가진 저장 패킷은 저장 패킷들 중에서 가장 나중에 수신된 패킷으로 가장 마지막 위치에 저장되게 되는데, 패킷 검출부(222)는 그 마지막 위치에 저장된 패킷을 기준 패킷으로서 검출하게 된다.

[0049] 비교부(224)는 기준 패킷과 현재 패킷의 시퀀스 번호 및 패킷 길이 값을 이용하여 패킷들을 비교한다.

[0050] 보다 구체적으로는, 비교부(224)는 기준 패킷의 시퀀스 번호와 현재 패킷의 시퀀스 번호가 일치하는지 여부를 판단한다.

[0051] 만일, 기준 패킷의 시퀀스 번호와 현재 패킷의 시퀀스 번호가 일치하면 비교부(224)는 시퀀스 번호가 일치함을 나타내는 비교 결과를 패킷 판단부(226)에게 전달한다.

[0052] 하지만, 기준 패킷의 시퀀스 번호와 현재 패킷의 시퀀스 번호가 일치하지 않으면, 기준 패킷의 시퀀스 번호와 패킷 길이 값을 합산한 합산 값이 현재 패킷의 시퀀스 번호보다 작은지 여부를 판단한 후, 그 비교 결과를 판단부(226)에게 전달한다.

[0053] 다른 실시예에서는, 비교부(224)가 패킷의 전송 방향, ACK 번호 등을 더 고려할 수도 있다.

[0054] 패킷 판단부(226)는 비교부(224)의 비교 결과에 기초하여, 현재 패킷이 제1 유형 패킷 또는 제2 유형 패킷인지 여부를 판단한다.

[0055] 만일, 비교부(224)로부터 전달받은 비교 결과가 기준 패킷의 시퀀스 번호와 현재 패킷의 시퀀스 번호가 일치한다는 것이라면 패킷 판단부(226)는 현재 패킷을 제1 유형 패킷으로 판단하고, 비교 결과가 기준 패킷의 시퀀스 번호와 패킷 길이 값을 합산한 합산 값이 현재 패킷의 시퀀스 번호보다 작다는 것이라면 패킷 판단부(226)는 현재 패킷을 제2 유형 패킷으로 판단한다. 또한, 현재 패킷이 제1 유형 패킷 또는 제2 유형 패킷 어디에도 해당하지 않는다고 판단되는 경우에는 패킷 판단부(226)는 현재 패킷을 일반 패킷으로 판단할 수 있다.

[0056] 패킷 판단부(226)가 현재 패킷을 제1 유형 패킷 또는 제2 유형 패킷으로 판단하면 패킷 처리부(230)는 그 제1 유형 패킷 또는 제2 유형 패킷으로 판단한 현재 패킷을 삭제하지만, 현재 패킷을 일반 패킷으로 판단하면 패킷 처리부(230)는 그 일반 패킷으로 판단한 현재 패킷은 저장하게 된다.

[0057] 도 4는 본 발명의 일 실시예에 따른 중복 패킷 발생을 방지하는 패킷 처리 방법을 설명하기 위하여 도시한 흐름도이다.

[0058] 단계 410에서는, 패킷 처리 장치(200)가 제1 호스트와 제2 호스트간에 전송되는 패킷들 중 하나를 현재 패킷으로서 수신한다.

[0059] 단계 420에서는, 패킷 처리 장치(200)가 현재 패킷을 현재 패킷 이전에 수신되어 저장된 저장 패킷들과 비교하여, 현재 패킷이 저장 패킷들 중 하나와 동일한 페이로드 값을 포함하는 제1 유형 패킷 또는 제1 유형 패킷과 관련된 패킷으로서 제1 유형 패킷 이후에 수신된 제2 유형 패킷인지 여부를 판단한다.

[0060] 패킷 처리 장치(200)가 현재 패킷이 제1 유형 패킷 또는 제2 유형 패킷인지 여부를 판단하는 동작에 대해서는 도 5를 참조하여 보다 구체적으로 설명한다.

[0061] 단계 430에서는, 패킷 처리 장치(200)가 그 판단에 기초하여, 현재 패킷을 선택적으로 삭제한다.

[0062] 도 5는 본 발명의 일 실시예에 따른 패킷 유형 판단 방법을 설명하기 위하여 도시한 흐름도이다.

[0063] 단계 510에서는, 패킷 처리 장치(200)가 현재 패킷의 전송 방향과 동일한 전송 방향의 저장 패킷들 중에서 가장 큰 시퀀스 번호를 가진 저장 패킷인 기준 패킷을 검출한다.

[0064] 단계 520에서는, 패킷 처리 장치(200)가 기준 패킷과 현재 패킷의 시퀀스 번호 및 패킷 길이 값을 이용하여 기준 패킷과 현재 패킷을 비교한다.

[0065] 단계 530에서는, 패킷 처리 장치(200)가 그 비교 결과에 기초하여, 현재 패킷이 제1 유형 패킷 또는 제2 유형 패킷인지 여부를 판단한다.

[0066] 도 6은 본 발명의 일 실시예에 따른 중복 패킷 발생을 방지하는 패킷 처리 방법에 대한 의사코드를 나타내는 도면이다.

[0067] 도 6을 참조하면, P(n)은 TCP 플로우상의 n번째 패킷을 나타내고, P(n).seq는 n번째 패킷의 시퀀스 번호를 나타내고, P(n).ack은 n번째 패킷의 ACK 번호를 나타내고, P(n).dir은 n번째 패킷의 전송 방향을 나타내고, P(n).len은 n번째 패킷의 패킷 길이(페이로드 길이) 값을 나타낸다.

[0068] 의사 코드의 첫 번째 줄은 본 의사 코드가 재전송에 따른 중복 패킷 문제를 해결하기 위한 처리 절차임을 나타낸다.

[0069] 두 번째 줄에서, n번째 패킷 P(n)이 현재 패킷으로서 수신된다.

[0070] 세 번째 줄에서, 현재 패킷 P(n)과 방향이 같고 현재 패킷 P(n)보다 먼저 수신된 저장 패킷들 중에서 가장 큰 시퀀스 번호를 가진 저장 패킷인 기준 패킷 P(k)를 검출한다.

[0071] 네 번째 줄에서, 현재 패킷 P(n)의 시퀀스 번호와 기준 패킷 P(k)의 시퀀스 번호가 동일한지 여부를 비교하여 현재 패킷 P(n)이 제1 유형 패킷인지 여부를 판단한다.

[0072] 다섯 번째 줄에서, 현재 패킷 P(n)이 제1 유형 패킷으로 판단되면 현재 패킷 P(n)을 삭제한다.

[0073] 여섯 번째 줄에서, 기준 패킷 P(k)의 시퀀스 번호와 패킷 길이 값을 합산한 합산 값이 현재 패킷 P(n)의 시퀀스 번호보다 작은지 여부를 비교하여 현재 패킷 P(n)이 제2 유형 패킷인지 여부를 판단한다.

[0074] 일곱 번째 줄에서, 현재 패킷 P(n)이 제2 유형 패킷으로 판단되면 현재 패킷 P(n)을 삭제한다.

[0075] 여덟 번째 줄에서, 모든 처리 절차를 종료한다.

[0076] 도 7은 본 발명의 일 실시예에 따른 중복 패킷 발생을 방지하는 패킷 처리 방법을 도 1의 트래픽 수집 지점 C2에 적용하여 설명하기 위하여 도시한 도면이다.

[0077] 도 7에서 빗금이 없는 패킷들은 호스트 A가 호트스 B에게 전송하는 순방향 패킷들을 나타내고, 빗금이 쳐진 패킷들은 호스트 B가 호스트 A에게 전송하는 역방향 패킷들을 나타내고, X표로 표시된 패킷들은 삭제되는 패킷들을 나타낸다.

[0078] 도 7의 실시예를 순차적으로 설명하면 다음과 같다.

[0079] 첫번째 단계에서, 저장 패킷들인 패킷 a 내지 패킷 g가 저장된 상태에서 h 패킷이 현재 패킷으로서 수신된다.

[0080] 두번째 단계에서, h 패킷과 동일한 전송 방향을 가진 저장 패킷들 중에서 가장 시퀀스 번호가 큰 패킷인 g 패킷이 기준 패킷으로 설정된다.

[0081] 세번째 단계에서, 기준 패킷 g 패킷의 시퀀스 번호와 h 패킷의 시퀀스 번호를 비교함으로써, h 패킷이 제1 유형 패킷인지 여부를 판단한다.

[0082] 네번째 단계에서, g 패킷과 h 패킷의 시퀀스 번호가 동일하여 h 패킷이 제1 유형 패킷으로 판단되어 h 패킷이 삭제된다.

[0083] 다섯번째 단계에서, i 패킷이 현재 패킷으로서 수신된다.

[0084] 여섯번째 단계에서, 기준 패킷 g 패킷의 시퀀스 번호와 i 패킷의 시퀀스 번호를 비교함으로써, i 패킷이 제1 유형 패킷인지 여부를 판단한다.

[0085] 일곱번째 단계에서, g 패킷과 i 패킷의 시퀀스 번호가 동일하여 i 패킷이 제1 유형 패킷으로 판단되어 i 패킷이 삭제된다.

[0086] 여덟번째 단계에서, 역방향 패킷인 j 패킷이 현재 패킷으로서 수신된다.

[0087] 아홉번째 단계에서, 역방향 패킷 j 패킷과 동일한 전송 방향을 가진 저장 패킷들 중에서 가장 시퀀스 번호가 큰 패킷인 d 패킷이 기준 패킷으로 설정된다.

[0088] 열번째 단계에서, 기준 패킷 d 패킷의 시퀀스 번호와 j 패킷의 시퀀스 번호를 비교함으로써, j 패킷이 제1 유형 패킷인지 여부를 판단한다.

[0089] 열한번째 단계에서, 기준 패킷 d 패킷의 시퀀스 번호와 j 패킷의 시퀀스 번호가 동일하지 않으므로, 기준 패킷 d 패킷의 시퀀스 번호와 패킷 길이 값을 합산한 값 80이 j 패킷의 시퀀스 번호 80보다 작은지를 판단하여 제2 유형 패킷인지 여부를 판단한다.

[0090] 열두번째 단계에서, 기준 패킷 d 패킷의 시퀀스 번호와 패킷 길이 값을 합산한 값 80이 j 패킷의 시퀀스 번호 80보다 작지 않으므로, j 패킷을 일반 패킷으로 판단하여 삭제하지 않고 저장한다.

[0091] 열세번째 단계에서, 역방향 패킷인 k 패킷이 현재 패킷으로서 수신된다.

[0092] 열네번째 단계에서, 역방향 패킷 k 패킷과 동일한 전송 방향을 가진 저장 패킷들 중에서 가장 시퀀스 번호가 큰 패킷인 j 패킷이 기준 패킷으로 설정된다.

[0093] 열다섯번째 단계에서, 기준 패킷 j 패킷의 시퀀스 번호와 k 패킷의 시퀀스 번호를 비교함으로써, k 패킷이 제1 유형 패킷인지 여부를 판단한다.

[0094] 열여섯번째 단계에서, j 패킷과 k 패킷의 시퀀스 번호가 동일하여 k 패킷이 제1 유형 패킷으로 판단되어 k 패킷이 삭제된다.

[0095] 마지막으로, l 패킷은 일반 패킷으로 판단하여 저장하고, m 패킷은 제2 유형 패킷으로 판단하여 삭제하게 되는데, l 패킷과 m 패킷에 대해서도 도 7의 첫번째 단계 내지 열여섯번째 단계와 동일한 프로세스가 적용되므로 상세한 설명은 생략한다.

[0096] 결과적으로, 도 7의 첫번째 단계 내지 열여섯번째 단계를 통해 g 패킷 이후에 저장되는 패킷들의 순서는 g-i-k-l 패킷의 순서가 되며, 중복 패킷은 저장되지 않게 된다.

[0097] 도 8은 본 발명의 일 실시예에 따른 중복 패킷 발생을 방지하는 패킷 처리 장치를 이용한 트래픽 분석 시스템을 설명하기 위하여 도시한 도면이다.

[0098] 도 8에서, 호스트 A(812)와 호스트 B(814) 상호간에 패킷들을 전송하는 중에, 트래픽 수집 지점인 라우터(820)가 중간에서 호스트 A(812)와 호스트 B(814) 상호간에 전송하는 패킷들을 수신하게 된다.

[0099] 트래픽 캡쳐 시스템(830)은 라우터에 수신된 패킷들을 수집하여 본 발명에 따른 패킷 처리 장치(840)에게 전송한다.

[0100] 본 발명에 따른 패킷 처리 장치(850)는 중복 패킷이 발생하지 않도록 처리된 패킷들을 트래픽 분석 시스템(850)에게 전송한다.

[0101] 트래픽 분석 시스템(850)은 중복 패킷이 발생하지 않도록 처리된 패킷들을 이용하여 통계 정보 시그니처를 만든다.

[0102] 다음으로, 트래픽 분석 시스템(850)이 패킷 처리 장치(850)로부터 중복 패킷이 발생하지 않도록 처리된 패킷들을 새롭게 수신하게 되면, 기존에 생성한 통계 정보 시그니처에 기초하여 그 수신된 패킷들을 분석하여 트래픽 분류 결과를 도출하게 된다. 예컨대, 트래픽 분석 시스템(850)은 패킷 처리 장치(850)를 통해 수신된 중복 패킷이 발생하지 않도록 처리된 패킷들을 분석하여 그 패킷들이 어떤 응용(application)으로부터 생성된 것인지에 따라 트래픽 분류를 수행할 수 있다.

[0103] 이와 관련하여, 특정 대학 연구실에서 2시간 동안의 트래픽 분석 실험을 수행한 결과에 따르면, 전체 플로우의 7.7% 및 전체 패킷의 2.45%에서 패킷 재전송이 발생한 것으로 파악되어, 약 2%~8%의 트래픽에 대해서는 그 트래픽이 어떤 응용에서 생성된 것인지 탐지하지 못하거나 상이한 응용에서 생성된 것으로 탐지하는 문제가 발생할 수 있음을 알 수 있었다. 이와 같은 경우에 본 발명에 따른 패킷 처리 방법을 적용하게 되면 트래픽 미탐지 및 오탐지 문제가 해결되므로 트래픽 분석 결과의 신뢰성이 향상될 수 있다.

[0104] 지금까지 본 발명의 실시예들은 트래픽 수집 지점에 역전 패킷이 발생하는 경우에 대해서 설명하였으나, 본 발명은 이에 한정되지 않고 트래픽 수집 지점 뿐만 아니라 패킷을 수신하는 최종단에 위치하는 호스트에도 적용될 수 있다.

[0105] 한편, 상술한 본 발명의 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성가능하고, 컴퓨터로 읽을 수 있는 기록매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

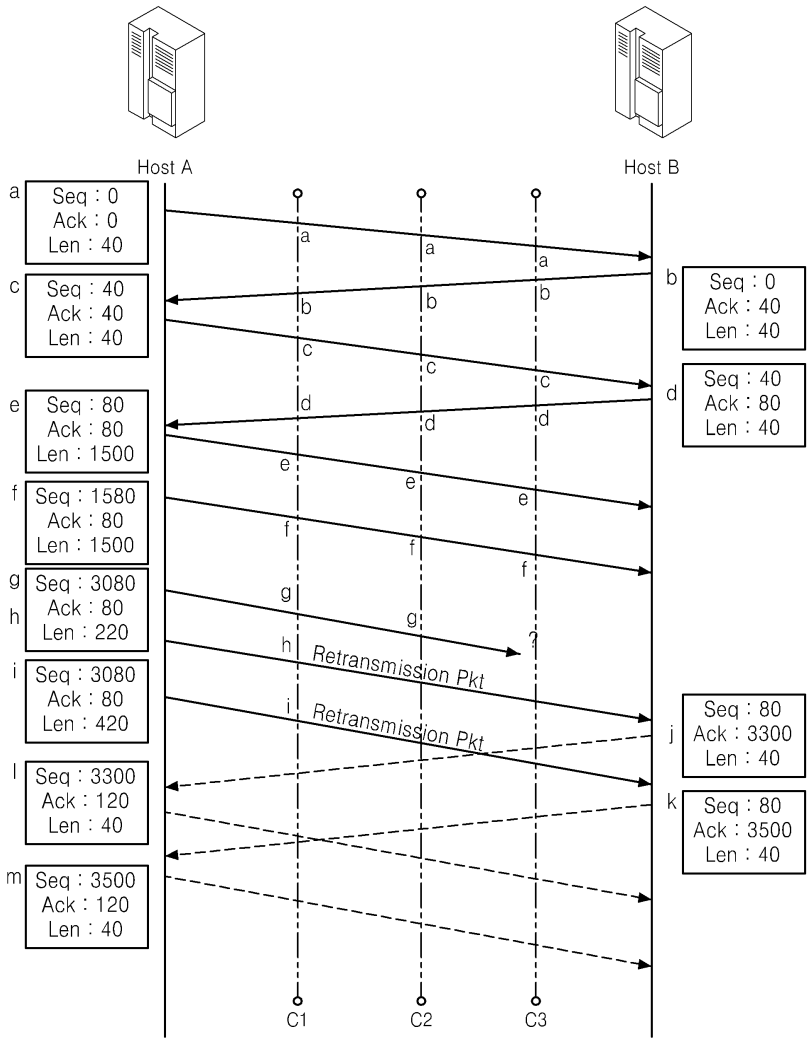
[0106] 상기 컴퓨터로 읽을 수 있는 기록매체는 마그네틱 저장매체(예를 들면, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등) 를 포함한다.

[0107] 이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현

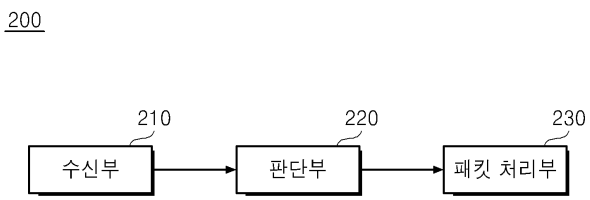
될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

도면

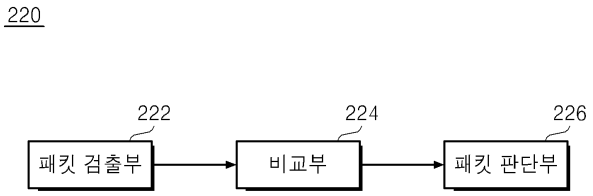
도면1



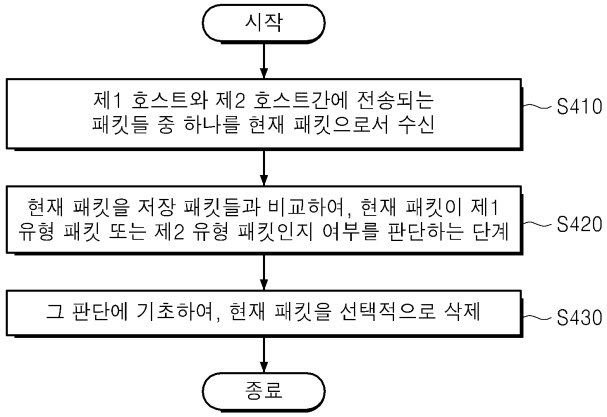
도면2



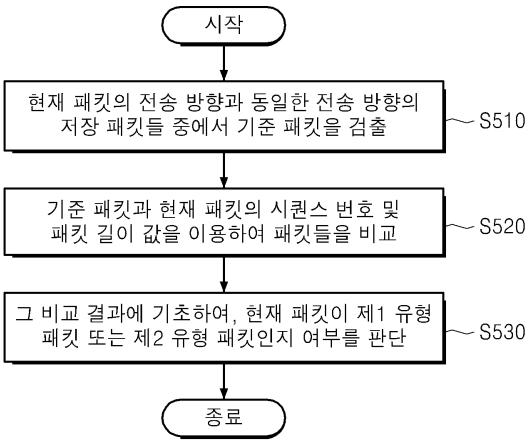
도면3


220
222
224
226
패킷 검출부
비교부
패킷 판단부

도면4


시작
제1 호스트와 제2 호스트간에 전송되는 패킷들 중 하나를 현재 패킷으로서 수신
S410
현재 패킷을 저장 패킷들과 비교하여, 현재 패킷이 제1 유형 패킷 또는 제2 유형 패킷인지 여부를 판단하는 단계
S420
그 판단에 기초하여, 현재 패킷을 선택적으로 삭제
S430
종료

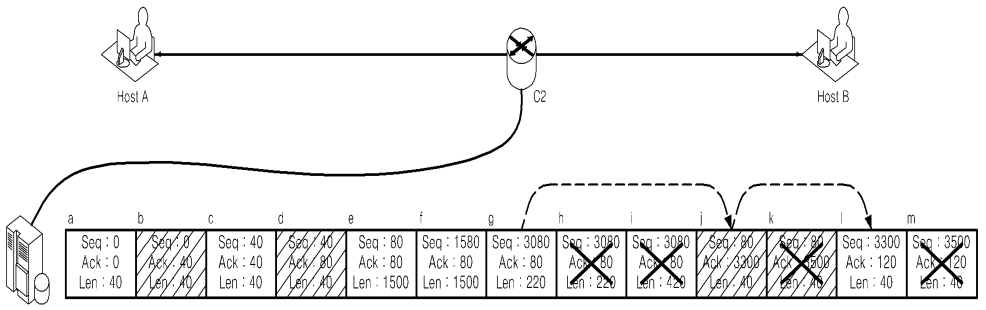
도면5


시작
현재 패킷의 전송 방향과 동일한 전송 방향의 저장 패킷들 중에서 기준 패킷을 검출
S510
기준 패킷과 현재 패킷의 시퀀스 번호 및 패킷 길이 값을 이용하여 패킷들을 비교
S520
그 비교 결과에 기초하여, 현재 패킷이 제1 유형 패킷 또는 제2 유형 패킷인지 여부를 판단
S530
종료

도면6

```
Remove all non-payload packets from the packet sequence
P(n) : n-th packet in a TCP flow
P(n).seq : n-th packet's sequence number
P(n).ack : n-th packet's acknowledge number
P(n).dir : n-th packet's direction
P(n).len : n-th packet's payload length
-----------------------------------------------------
1:  Procedure Solution for the Retransmission problem
2:  Input : P(n) in a TCP Flow
3:  find P(k) which P(k).dir == P(n).dir && biggest k in 0<=k < n;
4:  if(P(k).seq==P(n).seq) // Retransmission
5:      Delete P(n);
6:  else if ( P(k).seq + P(k).len < P(n).seq )
7:      Delete P(n);
8:  end procedure;
-----------------------------------------------------
```

도면7



도면8