(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년08월14일
(11) 등록번호 10-1428989
(24) 등록일자 2014년08월05일

(51) 국제특허분류(Int. Cl.)
H04L 12/26 (2006.01) *H04L 12/24* (2006.01)
(21) 출원번호 10-2013-0052154
(22) 출원일자 2013년05월08일
심사청구일자 2013년05월08일
(56) 선행기술조사문헌
JP2005073248 A*
KR1020020041002 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
김명섭
충청남도 연기군 조치원읍 신흥리 푸르지오아파트 111-902
김민석
대구 달성군 다사읍 대실역북로 16, 103동 603호 (죽곡청아람푸르지오1단지)
안현민
제주특별자치도 제주시 구남로2길 36 시엔제이빌 401호
(74) 대리인
특허법인엠에이피에스

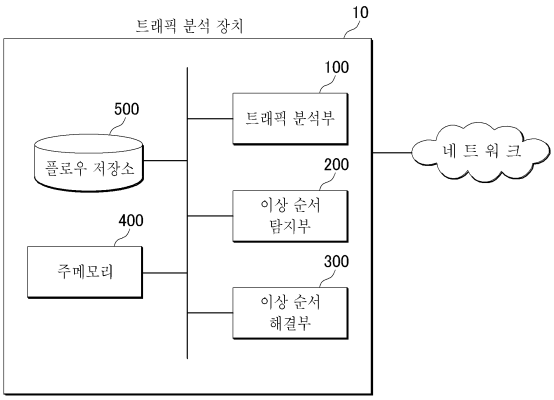
전체 청구항 수 : 총 4 항 심사관 : 전용해

(54) 발명의 명칭 **트래픽 분석 장치 및 방법**

(57) 요 약

본 발명은 네트워크로부터 수집한 트래픽 플로우를 저장하는 플로우 저장소; 상기 플로우 저장소에 저장되어 있는 트래픽 플로우의 순서가 비정상인지 여부를 판단하는 비정상 순서 탐지부; 상기 비정상 순서 탐지부에 의해 비정상으로 판단된 트래픽 플로우의 순서를 조정하는 비정상 순서 해결부; 및 상기 비정상 순서 해결부에 의해 순서가 조정된 트래픽 플로우를 사용하여 네트워크 트래픽 분석을 수행하는 트래픽 분석부;를 포함하되, 상기 비정상 순서 탐지부는 클라이언트-서버 간 트래픽 플로우에 대해, 상기 클라이언트가 상기 서버로 전송하는 트래픽 전송 방향을 포워드(포워드)로, 상기 서버가 상기 클라이언트로 전송하는 트래픽 전송 방향을 백워드(백워드)로 정의하고, 상기 트래픽 플로우의 트래픽 전송 방향이 포워드인지 백워드인지를 고려하여 비정상 여부를 판단하는 네트워크 트래픽 분석 장치를 제공한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

네트워크 트래픽 분석 장치에 있어서,

네트워크로부터 수집한 트래픽 플로우를 저장하는 플로우 저장소;

상기 플로우 저장소에 저장되어 있는 트래픽 플로우의 순서가 비정상인지 여부를 판단하는 이상 순서 탐지부;

상기 이상 순서 탐지부에 의해 비정상으로 판단된 트래픽 플로우의 순서를 조정하는 이상 순서 해결부; 및

상기 이상 순서 해결부에 의해 순서가 조정된 트래픽 플로우를 사용하여 네트워크 트래픽 분석을 수행하는 트래픽 분석부;를 포함하되,

상기 이상 순서 탐지부는

클라이언트-서버 간 트래픽 플로우에 대해, 상기 클라이언트가 상기 서버로 전송하는 트래픽 전송 방향을 포워드(forward)로, 상기 서버가 상기 클라이언트로 전송하는 트래픽 전송 방향을 백워드(backward)로 정의하고,

상기 트래픽 플로우의 트래픽 전송 방향이 포워드인지 백워드인지 여부, 및 상기 수집한 트래픽 플로우의 순서가 상기 수집한 트래픽 플로우의 클라이언트에서 송수신하는 순서와 일치하는지 여부에 따라 비정상 여부를 판단하며,

상기 이상 순서 해결부는 상기 비정상으로 판단된 트래픽 플로우의 순서를 상기 수집한 트래픽 플로우의 클라이언트에서 송수신하는 순서와 일치시키는 것인 네트워크 트래픽 분석 장치.

청구항 2

제 1 항에 있어서,

상기 이상 순서 탐지부는

페이로드를 포함하고 있는 TCP 패킷에 대해, 상기 TCP 패킷이 포함하는 Seq 및 Ack 정보를 사용하여 비정상 여부를 판단하는 네트워크 트래픽 분석 장치.

청구항 3

삭제

청구항 4

네트워크 트래픽 분석 장치를 사용하는 네트워크 트래픽 분석 방법에 있어서,

(a) 네트워크로부터 수집한 트래픽 플로우의 순서가 비정상인지 여부를 판단하는 단계;

(b) 상기 (a) 단계에 의해 비정상으로 판단된 트래픽 플로우의 순서를 조정하는 단계; 및

(c) 상기 (b) 단계에 의해 순서가 조정된 트래픽 플로우를 사용하여 네트워크 트래픽 분석을 수행하는 단계;를 포함하되,

상기 (a) 단계는

클라이언트-서버 간 트래픽 플로우에 대해, 상기 클라이언트가 상기 서버로 전송하는 트래픽 전송 방향을 포워드(forward)로, 상기 서버가 상기 클라이언트로 전송하는 트래픽 전송 방향을 백워드(backward)로 정의하는 단계; 및

상기 트래픽 플로우의 트래픽 전송 방향이 포워드인지 백워드인지 여부, 및 상기 수집한 트래픽 플로우의 순서가 상기 수집한 트래픽 플로우의 클라이언트에서 송수신하는 순서와 일치하는지 여부에 따라 비정상 여부를 판단하는 단계를 포함하며,

상기 (b) 단계는 상기 비정상으로 판단된 트래픽 플로우의 순서를 상기 수집한 트래픽 플로우의 클라이언트에서

송수신하는 순서와 일치시키는 단계를 포함하는 네트워크 트래픽 분석 방법.

청구항 5

제 4 항에 있어서,

상기 (a) 단계는

페이로드를 포함하고 있는 TCP 패킷에 대해, 상기 TCP 패킷이 포함하는 Seq 및 Ack 정보를 사용하여 비정상 여부를 판단하는 네트워크 트래픽 분석 방법.

청구항 6

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 트래픽 분석 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 최근 인터넷의 급격한 발전으로 인해 효율적인 네트워크 관리를 위한 네트워크 트래픽 데이터 분석의 중요성이 강조되고 있다. 인터넷 사용자의 증가와 고속 네트워크의 보급으로 인해 네트워크 트래픽이 급증하고 있으며, 트래픽의 종류 또한 다양해지고 있다. 따라서 급증하는 인터넷 트래픽을 효과적으로 관리하기 위해 다양한 트래픽 분석 방법이 개발되고 있다.

[0003] 특히 응용 수준에서의 트래픽 분석은 네트워크의 효율적인 운영과 안정적인 서비스를 제공하기 위한 필수적인 요소이다. 응용 수준에서의 트래픽 분석을 위해서 플로우 통계 정보에 기반한 트래픽 분류 방법들이 제안되고 있다. 통계 정보로는 패킷 전송 순서, 패킷 전송 방향, 패킷 크기 등을 이용한다.

[0004] 하지만 트래픽 수집 지점의 차이로 인해서 트래픽이 통계 정보의 일관성을 잃게 되어 분석 결과를 신뢰할 수 없게 될 수 있다. 특히 트래픽의 중간 지점에서 패킷이 송신지에서의 전송 순서대로 수집되지 않았을 때 이를 그대로 통계 분석에 사용할 경우 잘못된 결과가 산출될 수 있다.

[0005] 따라서 트래픽 분석 결과의 신뢰성을 보장하기 위해서는 트래픽 수집 지점의 차이로 인하여 트래픽이 일관성을 잃게되는 문제를 해결할 필요가 있다.

[0006] 이와 관련하여 한국등록특허 10-1228640호("프래그먼트 필터링 방법")에는 라우터에서 수신한 프래그먼트를 재순서화하는 구성이 개시되어 있다.

[0007] 또한, 한국공개특허 10-2012-0102722호("데이터 패킷들을 판독 및 순서화하는 복수의 분석 수단을 동작시키는 장치, 어셈블리, 및 방법")에는 수신한 패킷을 순서화하여 출력하는 구성이 개시되어 있다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 전술한 문제를 해결하기 위한 것으로서, 그 목적은 올바른 패킷 순서를 보장하는 트래픽 분석 장치 및 방법을 제공하는 것이다.

과제의 해결 수단

[0009] 상기와 같은 목적을 달성하기 위한 본 발명의 제 1 측면에 따른 네트워크 트래픽 분석 장치는 네트워크로부터 수집한 트래픽 플로우를 저장하는 플로우 저장소; 상기 플로우 저장소에 저장되어 있는 트래픽 플로우의 순서가 비정상인지 여부를 판단하는 비정상 순서 탐지부; 상기 비정상 순서 탐지부에 의해 비정상으로 판단된 트래픽 플로우의 순서를 조정하는 비정상 순서 해결부; 및 상기 비정상 순서 해결부에 의해 순서가 조정된 트래픽 플로우를 사용하여 네트워크 트래픽 분석을 수행하는 트래픽 분석부;를 포함하되, 상기 비정상 순서 탐지부는 클라이언트-서버 간 트래픽 플로우에 대해, 상기 클라이언트가 상기 서버로 전송하는 트래픽 전송 방향을 포워드(포

워드)로, 상기 서버가 상기 클라이언트로 전송하는 트래픽 전송 방향을 백워드(백워드)로 정의하고, 상기 트래픽 플로우의 트래픽 전송 방향이 포워드인지 백워드인지를 고려하여 비정상 여부를 판단하는 것을 특징으로한다.

[0010] 상기와 같은 목적을 달성하기 위한 본 발명의 제 2 측면에 따른 네트워크 트래픽 분석 장치를 사용하는 네트워크 트래픽 분석 방법은 (a) 네트워크로부터 수집한 트래픽 플로우의 순서가 비정상인지 여부를 판단하는 단계; (b) 상기 (a) 단계에 의해 비정상으로 판단된 트래픽 플로우의 순서를 조정하는 단계; 및 (c) 상기 (b) 단계에 의해 순서가 조정된 트래픽 플로우를 사용하여 네트워크 트래픽 분석을 수행하는 단계;를 포함하되, 상기 (a) 단계는 클라이언트-서버 간 트래픽 플로우에 대해, 상기 클라이언트가 상기 서버로 전송하는 트래픽 전송 방향을 포워드(포워드)로, 상기 서버가 상기 클라이언트로 전송하는 트래픽 전송 방향을 백워드(백워드)로 정의하고, 상기 트래픽 플로우의 트래픽 전송 방향이 포워드인지 백워드인지를 고려하여 비정상 여부를 판단하는 것을 특징으로한다.

발명의 효과

[0011] 본 발명은 트래픽 분석 장치 및 방법의 신뢰성을 보장하는 효과를 얻는다.

[0012] 트래픽 분석을 위해 수집한 패킷의 순서 일관성을 유지함으로써, 통계 정보 기반 트래픽 분류 결과의 신뢰성을 보장 할 수 있다. 특히 본 발명은 트래픽 수집 지점에 따라 트래픽 특징값(feature)이 달라지는 TCP 세션의 이상 동작 중 하나인 비정상 순서(cross-order) 문제를 해결한다. 본 발명은 수집한 트래픽을 송신지에서 전송한 순서, 예를 들어, 클라이언트에서 송수신하는 순서에 따라 재정렬하여 이러한 효과를 얻는다.

도면의 간단한 설명

[0013] 도 1은 본 발명의 일실시예에 따른 트래픽 분석 장치의 구조를 도시함.

도 2는 종래의 트래픽 분석 방법의 실시예를 도시함.

도 3은 본 발명의 일실시예에 따른 트래픽 분석 방법의 흐름을 도시함.

도 4는 본 발명의 일실시예에 따른 비정상 순서 탐지 방법의 실시예를 도시함.

도 5는 본 발명의 일실시예에 따른 비정상 순서 해결 방법의 실시예를 도시함.

도 6은 본 발명의 일실시예에 따른 비정상 순서 탐지 방법에 의해 정상적으로 판단되는 예를 도시함.

도 7 내지 도 9는 본 발명의 일실시예에 따른 비정상 순서 탐지 방법에 의해 비정상적으로 판단되는 예를 도시함.

발명을 실시하기 위한 구체적인 내용

[0014] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0015] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0016] 도 1은 본 발명의 일실시예에 따른 트래픽 분석 장치의 구조를 도시하고 있다.

[0017] 본 발명의 일실시예에 따른 트래픽 분석 장치(10)은 트래픽 분석부(100), 비정상 순서 탐지부(200), 비정상 순서 해결부(300), 주메모리(400), 및 플로우 저장소(500)를 포함한다.

[0018] 플로우 저장소(500)는 네트워크로부터 수집한 트래픽 플로우를 저장하며, 수집된 트래픽 플로우는 주메모리(400)에 적재되어 분석된다. 이러한 트래픽 분석을 수행하는 것은 트래픽 분석부(100)이다. 그러나 수집된 트래픽 플로우는 송신지에서 전송한 순서에 따라 수집되지 않을 수 있으므로, 트래픽 분석부(100)가 트래픽 분석을 수행하기 전에 먼저 이상 순서 탐지부(200)가 수집된 트래픽 플로우의 순서가 비정상인지 여부를 판단하고, 이

상 순서 해결부(300)가 비정상으로 판단된 트래픽 플로우의 순서를 조정한다.

[0019] 자세한 내용을 이하 도 2 내지 도 9를 통해 살펴본다.

[0020] 도 2는 종래의 트래픽 분석 방법의 실시예를 도시하고 있다.

[0021] 트래픽 분석 방법은 네트워크 트래픽을 응용 프로그램별 분류하는 것으로, 이를 위해 다양한 방법들이 제시되어 왔다. 이러한 종래 기술들은 크게 3가지로 구분할 수 있는데, 시그니쳐 기반 분석 기법, 트래픽 상관 관계 기반 분석, 및 머신 러닝 기반 분석이다. 시그니쳐 기반 분석 방법에는 통계 시그니쳐 기반 분석 방법이 있으며, 이는 머신 러닝 기반 분석 방법과 결합되어 사용될 수 있다.

[0022] 통계 시그니쳐 기반 트래픽 분석 방법은 TCP 또는 UDP를 전송 프로토콜로 사용하는 네트워크 트래픽 플로우(network traffic flow)를 입력으로 받으며, 플로우 내의 제어 패킷을 제외한 페이로드(payload)가 있는 패킷(packet)만을 분석 대상으로 삼아, 이들의 특징값(feature)을 트래픽 분석에 사용한다.

[0023] 예를 들어, 먼저 플로우의 첫 N개 패킷의 페이로드 크기와 전송 방향, 순서를 이용하여 N차원의 플로우 벡터로 표현한다. 플로우 벡터에서 패킷의 페이로드 크기는 정수로 표현되고, 전송방향은 TCP의 경우 "양"은 클라이언트에서 서버로 향하는 패킷, "음"은 서버에서 클라이언트로 향하는 패킷을 의미할 수 있다. UDP는 클라이언트와 서버의 구분이 명확하지 않기 때문에 발생되는 첫 패킷을 "양"으로 표현하고 뒤에 이어지는 패킷은 첫 패킷을 기준으로 방향이 같으면 "양", 다르면 "음"으로 표현할 수 있다.

[0024] 플로우 벡터는 V(f)={d1xs1, d2xs2, ..., dnxsn}으로 표현할 수 있다. 이때 f는 플로우, V(f)는 플로우 f의 벡터, di는 플로우 f 내 i 번째 패킷의 전송 방향(양 또는 음), si는 i 번째 패킷의 페이로드 크기를 의미하며, 각 요소의 순서는 플로우 내 패킷의 전송 순서이다.

[0025] 예를 들어 두 종단 호스트 A와 B가 통신을 하는데 A가 먼저 B에게 데이터 크기가 30인 패킷을 두 개 연속으로 보내고 B에서 A로 데이터 크기 40인 패킷을 하나 전송한다면 두 종단호스트를 연결하는 플로우 f 의 벡터 V(f)는 V(f)= {+30, +30, -40}으로 표현할 수 있다.

[0026] 통계 시그니쳐 기반 분석 방법은 이렇게 표현된 N차원의 플로우 벡터를 사용하여 추출된 시그니쳐와 비교, 분석한다.

[0027] 이렇게 패킷 전송 순서, 패킷 전송 방향, 패킷 크기 등을 특징값으로 이용하는 통계 시그니쳐 기반 분석은 트래픽 수집 지점에 따라 특징값 중 하나인 패킷 순서의 값이 달라지게되는 문제에 의해 결과의 신뢰성을 손상받을 수 있다.

[0028] 예를 들어, TCP에서 두 호스트에서 통신 중일 때 한 종점 호스트에서 전송되는 패킷을 기다리지 않고 상대 호스트에서 동시에 패킷을 발생시키는 경우가 있는데 이때 트래픽 수집 지점에 따라 플로우의 통계 정보가 변하게된다. 즉, 통계 정보를 특징값로 사용하는 트래픽 분석 방법론은 수집 지점의 차이로 인해 일정한 특징값를 보장받지 못하며 분석 결과를 신뢰할 수 없다. 이러한 특징값 중 하나인 패킷 순서는 트래픽 수집 지점에 따라 달라지게된다. 이를 본 명세서에서는 비정상 순서(cross-order)라고 정의한다.

[0029] 예를 들면 도면에 도시되어 있는 바와 같이, 두 종단 호스트, 즉, 클라이언트(client)와 서버(server)가 서로 통신할 때, 트래픽 수집 지점인 C1, C2, C3, C4에 따라 패킷의 순서가 달라지고 또한 통계 정보가 달라진다. 예를 들어, 클라이언트가 전송한 두 번째 패킷인 Seq 값이 20이고 Ack 값이 0인 패킷인 경우, 서버, C4, 및 C3에서는 서버가 전송한 첫 번째 패킷인 Seq 값이 0이고 Ack 값이 0인 패킷보다 먼저 수집되나, C2 및 C1에서는 나중에 수집된다.

[0030] 이러한 비정상 순서 문제로 인해 같은 플로우에서 특징값의 값이 달라져 일관성을 잃은 잘못된 분석을 하게되는 문제가 발생한다. 따라서, 본 발명의 일실시예에 따른 트래픽 분석 장치(10) 및 방법은 트래픽 분석 전에 수집한 패킷의 순서를 송신지에서 전송한 순서(예: 클라이언트에서 송수신하는 순서)에 따라 재조정하는 과정을 거친다.

[0031] 즉, 도시된 바와 같이, 트래픽 수집 지점 C1, C2, C3, C4는 동일한 플로우를 서로 다른 순서로 수집한다. 이를 일관성있는 순서로 재조정하여 트래픽 분석 결과의 일관성을 보장하는 것이 본 발명의 목적이다.

[0032] 명확한 기준이 없으면 어느 것이 옳은 순서인지 잘못된 순서인지 알 수가 없으므로, 본 명세서는 클라이언트를 기준으로 전송 방향을 정한다. 클라이언트 기준이라는 것은 클라이언트가 패킷을 보내고 받는 순서를 일컫는 것이다. 클라이언트 기준인 이유는 대부분의 트래픽이 클라이언트에서 서버로 요청함에 따라 시작되어 서버에서

이에 응답하는 형식으로 이어지기 때문이다. 즉, 클라이언트의 요청에 따라 트래픽이 변화하기 때문이다.

[0033] 따라서 본 발명의 일실시예에 따른 트래픽 분석 장치(10)는 트래픽 수집 지점에 상관없이 클라이언트 기준으로 재정렬하며, 본 명세서는 포워드(forward) 패킷은 클라이언트에서 서버로 전송하는 패킷으로, 백워드(backward) 패킷은 서버에서 클라이언트로 전송하는 패킷으로 정의한다.

[0034] 또한 각 패킷 간의 교차(cross)를 클라이언트와 서버간의 포워드 패킷과 백워드 패킷의 전송 도중 수집 지점의 시점에 보았을 때 두 패킷이 만나는 것을 나타내는 용어로 사용한다. 즉, 포워드 패킷이든 백워드 패킷 중 어느 것이든 먼저 전송을 시작하였고 그 패킷이 상대 호스트에게 도착 전에 반대방향의 패킷이 전송을 하는 도중 겹치는 현상을 나타낸다.

[0035] 예를 들어, 앞서 설명한 예에서 클라이언트가 전송한 두 번째 패킷은 포워드 패킷이고, 서버가 전송한 첫번째 패킷은 백워드 패킷으로, C1 및 C2에서 이들을 수집하기 전에 교차되었기 때문에, 이들 트래픽 수집 지점에서는 클라이언트 또는 서버가 전송한 순서와는 다른 순서로 수집된 것이다.

[0036] 도 3은 본 발명의 일실시예에 따른 트래픽 분석 방법의 흐름을 도시하고 있다.

[0037] 일련의 트래픽 플로우에 대하여, 마지막 패킷(S800)에 이르기까지, 각 패킷 데이터에 대하여(S100), 패킷 인덱스 n을 1로 추기화한 후(S200), 다음 단계들을 반복한다.

[0038] 먼저, 이상 순서 탐지부(200)는 이상 순서 탐지 단계로 P(n)과 P(n+1)을 비교하여(S300) 이상 순서 여부를 판단한다(S400). 여기서 P(n)은 n 번째 패킷을 나타낸다. 즉, P(n)과 P(n+1)을 비교한다는 것은 일련의 트래픽 플로우의 각 패킷을 다음 패킷과 비교한다는 것이다.

[0039] 다음, 이상 순서인 것으로 판단되면 이상 순서 해결부(300)는 다음의 일련의 단계로 구성되는 이상 순서 해결 단계를 수행한다.

[0040] n이 1이 될 때까지, 즉, 트래픽이 0부터 시작된다고 가정했을 때 n이 0이 되기 전까지(S700), n을 감소시키면서(S600), P(n)과 P(n+1)의 순서를 서로 바꾼다(S500). 이때 이 과정은 P(n)과 P(n+1)을 비교한 결과(S300) 이상 순서가 아니라고 판단되는 경우에는(S400) 중지된다.

[0041] 자세한 내용은 해당 단계를 좀더 상세히 도시한 도 4 내지 도 5를 통해 설명한다.

[0042] 도 4는 본 발명의 일실시예에 따른 비정상 순서 탐지 방법의 실시예를 도시하고 있다.

[0043] 먼저, TCP 트래픽에 대해 전처리 과정을 거친다. 즉, 패킷 재전송(retransmission), 패킷 순서 엉킴(out-of-order) 문제가 제거된 TCP 트래픽을 추려낸 후, 그중에서 페이로드가 있는 패킷만을 입력으로 받는다. 즉, 제어 패킷은 트래픽 분석 대상으로 하지 않는다.

[0044] 도시된 알고리즘에서 P(n)은 n 번째 패킷을 가리키며 P(n)(Seq) 및 P(n)(Ack)는 각각 n 번째 패킷의 시퀀스 번호(sequence number) 즉, Seq 값 및 응답 번호(acknowledge number), 즉, Ack 값을 가리킨다.

[0045] P(n)의 Seq 값 및 Ack 값과 P(n+1)의 Seq값 및 Ack 값을 비교하여, 각각 4가지 경우에 따라 정상 순서과 비정상 순서 여부를 판단한다. 본 명세서는 이들을 정상 순서는 n.1 내지 n.4, 비정상 순서는 a.1 내지 a.4로 나타낸다.

[0046] 각 경우에 대한 자세한 내용은 이하 정상 순서인 경우 및 비정상 순서인 경우를 나타내는 도 6 내지 도 9를 통해 후술한다.

[0047] 도 5는 본 발명의 일실시예에 따른 비정상 순서 해결 방법의 실시예를 도시하고 있다.

[0048] 도면은 비정상 순서 문제가 탐지되었을 경우 이를 해결하는 알고리즘을 도시하고 있다. 수집된 트래픽을 가지고 탐지 알고리즘에 의해 탐지가되면 해결 알고리즘에 의해 n 번째 패킷과 n+1 번째 패킷의 순서를 바꿔준다.

[0049] 패킷의 교차가 한번만 일어난 경우에는 n 번째 패킷과 n+1 번째의 두 패킷 간의 패킷 순서만 바꾸면되지만, 패킷의 교차가 연속적일 경우에는, 즉, n+1 번째 패킷이 n 번째, n-1 번째 등 n 번째보다 이전의 패킷들과의 교차가 있다면, n 번째 패킷뿐만 아니라 이전 패킷들과도 패킷 순서 교체를 해주어야 한다.

[0050] 따라서 n 번째 패킷과 n+1 번째 패킷의 순서가 비정상이라고 탐지된 경우, n 번째와 n+1 번째 패킷의 순서를 교체하고, n 번째 시퀀스가 된 백워드 패킷은 n-1 번째 패킷과 비교하여 비정상이라고 탐지되면 교체하고, n-1 번째 시퀀스가 된 백워드 패킷은 n-2 번째 패킷과 비교하여 비정상이라고 탐지되면 교체하는 방식으로 비정상 순

서가 더이상 탐지되지 않을 때까지 역순으로 계속 수행한다.

[0051] 비정상 순서가 더이상 탐지되지 않는다면 n+1 번째 패킷으로 돌아가 다시 탐지를 수행하며 비정상 순서가 탐지되면 교체하는 반복적인 방법으로 전체 트래픽의 마지막 플로우까지 수행한다.

[0052] 도 6은 본 발명의 일실시예에 따른 비정상 순서 탐지 방법에 의해 정상적으로 판단되는 예를 도시하고 있다.

[0053] 정상 순서 1인 n.1은 n 번째 패킷과 n+1 번째 패킷이 같은 방향일 때, 정상 순서 2인 n.2는 n 번째 패킷이 포워드 패킷이고 n+1 번째 패킷이 백워드 패킷일 때의 경우이다.

[0054] n 번째 패킷과 n+1 번째 패킷이 같은 방향인 경우가 정상 순서로 판단되는 것은 당업자에게 쉽게 이해될 것이다. 재전송되거나 순서가 뒤엉킨 TCP 패킷을을 제거하는 전처리 과정을 거쳤기 때문에, 같은 방향으로 연이어 전송된 두 패킷은 수신지 뿐 아니라 중간 지점들에서도 송신지에서 전송한 순서, 즉, 클라이언트에서 송수신하는 순서 그대로 수신된다.

[0055] n 번째 패킷이 포워드 패킷인 경우도 항상 정상 순서이다. 도면에 도시되어 있는 바와 같이, 트래픽 수집 지점이 달라도 클라이언트에서의 기준으로는 모두 동일한 순서로 수집된다.

[0056] 이는 트래픽 수집 지점에 따라 패킷의 순서가 변화가되기 위해서는 포워드 패킷과 백워드 패킷이 두 패킷 중 하나 이상의 패킷이 반대 방향의 패킷이 도착하기 전보다 먼저 전송을 시작하여 서로 교차되는 것이 원인이며, 기준점으로 정한 클라이언트에서 보내고 받는 순서로 모든 트래픽 수집 지점에서의 패킷 순서를 맞춰주는 것이 본 발명의 목표이기 때문이다.

[0057] 포워드 패킷이 n 번째 패킷으로 수집되는 경우, 교차가 일어나려면 백워드 패킷이 포워드 패킷이 도착하기 전에 전송되어 교차가 일어나야 하기 때문에, 포워드 패킷이 n 번째로 수집된다면 항상 정상 순서가 된다.

[0058] 따라서 정상 순서 1, 2를 제외한 나머지 모든 경우는 P(n) 번째 패킷이 백워드 패킷이고 P(n+1) 번째 패킷이 포워드 패킷일 경우이다.

[0059] 정상 순서 3인 n.3은 n 번째 패킷이 백워드 패킷이지만 포워드 패킷과 백워드 패킷간의 교차가 없어 어느 지점에서 트래픽을 수집하든 패킷 순서에 영향을 미치지 않는 경우이다.

[0060] 정상 순서 4인 n.4와 같은 경우에는 n.4가 탐지되기 전 패킷 비교에서 포워드 패킷과 백워드 패킷이 교차하여 비정상 순서가 발생한다. 즉, n.4가 일어나기 전에는 항상 비정상 순서의 하나인 a.1이 먼저 발생한다. 즉, 정상 순서 4는 비정상 순서 1이 일어난 후에 발생되는 정상 순서로서, n 번째 패킷이 백워드 패킷이고 n+1 번째 패킷이 포워드 패킷인 경우이다. 이때 정상 순서 4와 비정상 순서 1은 각 패킷의 seq 값, ack 값의 비교를 통해 정상 순서과 비정상 순서로 판단한다.

[0061] 이처럼 정상 순서와 비정상 순서는 함께 발생할 수 있으며 트래픽 수집 지점에 따라 클라이언트 기준의 순서와 같을 수 있고 다를 수 있다.

[0062] 도 7 내지 도 9는 본 발명의 일실시예에 따른 비정상 순서 탐지 방법에 의해 비정상적으로 판단되는 예를 도시하고 있다.

[0063] 도 7은 비정상 순서 1 및 2인 a.1과 a.2를 나타낸다.

[0064] 비정상 순서 a.1는 전술한 바와 같이, n 번째 패킷이 백워드 패킷이고, n+1 번째 패킷이 포워드 패킷인 경우에서 백워드 패킷과 포워드 패킷이 각각 하나의 패킷이 교차가 일어났을 경우이다. 이 경우, C1과 C2에서 트래픽을 수집하였을 때는 문제가 되지 않지만, C3에서 트래픽 수집을 하였을 경우 클라이언트 기준의 순서와 동일하지 않게 되므로 비정상 순서가 된다.

[0065] 비정상 순서 a.1을 제외한 나머지 비정상 순서의 경우들, 즉, a.2, a.3, a.4는 모두 포워드 패킷 또는 백워드 패킷이 여러 번 교차하였을 때 발생한다.

[0066] 비정상 순서 2인 a.2 는 하나의 포워드 패킷이 도착하기 전에 백워드 패킷이 2개 이상의 패킷을 전송하여 교차가 발생하였을 때 일어나는 경우이다. 포워드 패킷이 전송된 후 수신지에 도착하기 전에 첫번째 교차가 일어나는 백워드 패킷 이후에 전송되고 포워드 패킷과 교차가 있는 모든 백워드 패킷에서 a.2는 탐지된다. 즉, a.2은 a.1이 먼저 탐지되고 난 후에 항상 발생할 수 있다.

[0067] 도 8은 비정상 순서 3인 a.3을 나타낸다.

[0068] a.2와 반대로 비정상 순서 3인 a.3은 하나의 백워드 패킷이 도착하기 전에 여러 개의 포워드 패킷이 2개 이상의 패킷을 전송하여 교차가 일어날 경우 탐지된다. 백워드 패킷이 전송되고 도착하기 전에 첫 번째 교차가 일어나는 포워드 패킷 이후에 전송되고 백워드 패킷과 교차가 있는 모든 포워드 패킷에서 a.3은 탐지된다. 즉, a.3 또한 a.1이 먼저 탐지되고 난 후에 항상 발생할 수 있다고 할 수 있다.

[0069] 도 9는 비정상 순서 4인 a.4를 나타낸다.

[0070] 비정상 순서 4인 a.4는 포워드 패킷과 백워드 패킷 모두 두 개 이상의 패킷이 교차될 때 탐지되는 경우이다. 즉, a.4는 a.1, a.2, a.3이 모두 발생한 후에 발생할 수 있고 교차된 마지막 포워드 패킷과 백워드 패킷에서 탐지된다.

[0071] 본 발명의 일 실시예는 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독 가능 매체는 컴퓨터 저장 매체 및 통신 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다. 통신 매체는 전형적으로 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조된 데이터 신호의 기타 데이터, 또는 기타 전송 메커니즘을 포함하며, 임의의 정보 전달 매체를 포함한다.

[0072] 본 발명의 방법 및 시스템은 특정 실시예와 관련하여 설명되었지만, 그것들의 구성 요소 또는 동작의 일부 또는 전부는 범용 하드웨어 아키텍처를 갖는 컴퓨터 시스템을 사용하여 구현될 수 있다. 본 발명의 일 실시예의 하나 이상의 구성 요소 또는 동작을 실시하기 위하여 사용될 수 있는 컴퓨터 시스템 아키텍처의 일례를 설명하면, 하드웨어 시스템은 프로세서, 캐쉬, 메모리 및 상술한 기능에 관련된 하나 이상의 소프트웨어 어플리케이션 및 드라이버를 포함할 수 있다.

[0073] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0074] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

[0075] 10: 트래픽 분석 장치

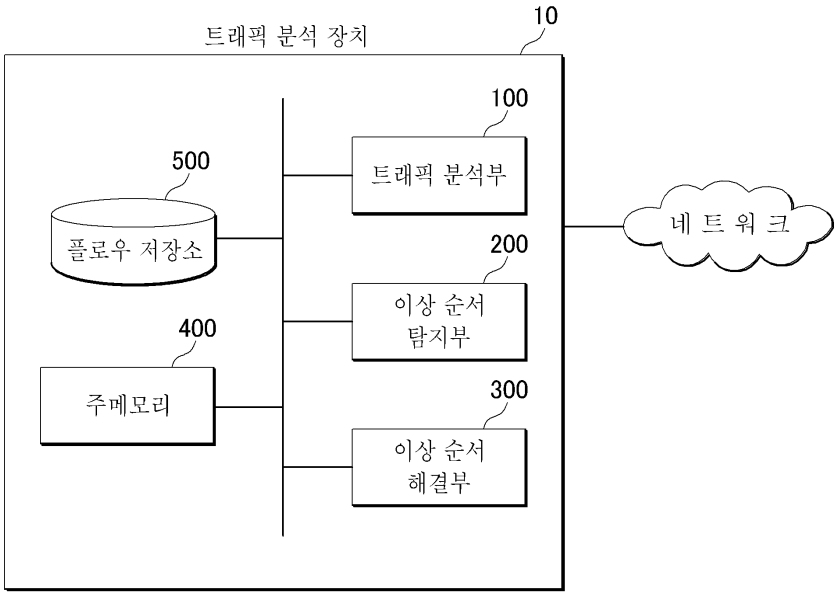
100: 트래픽 분석부

200: 비정상 순서 탐지부

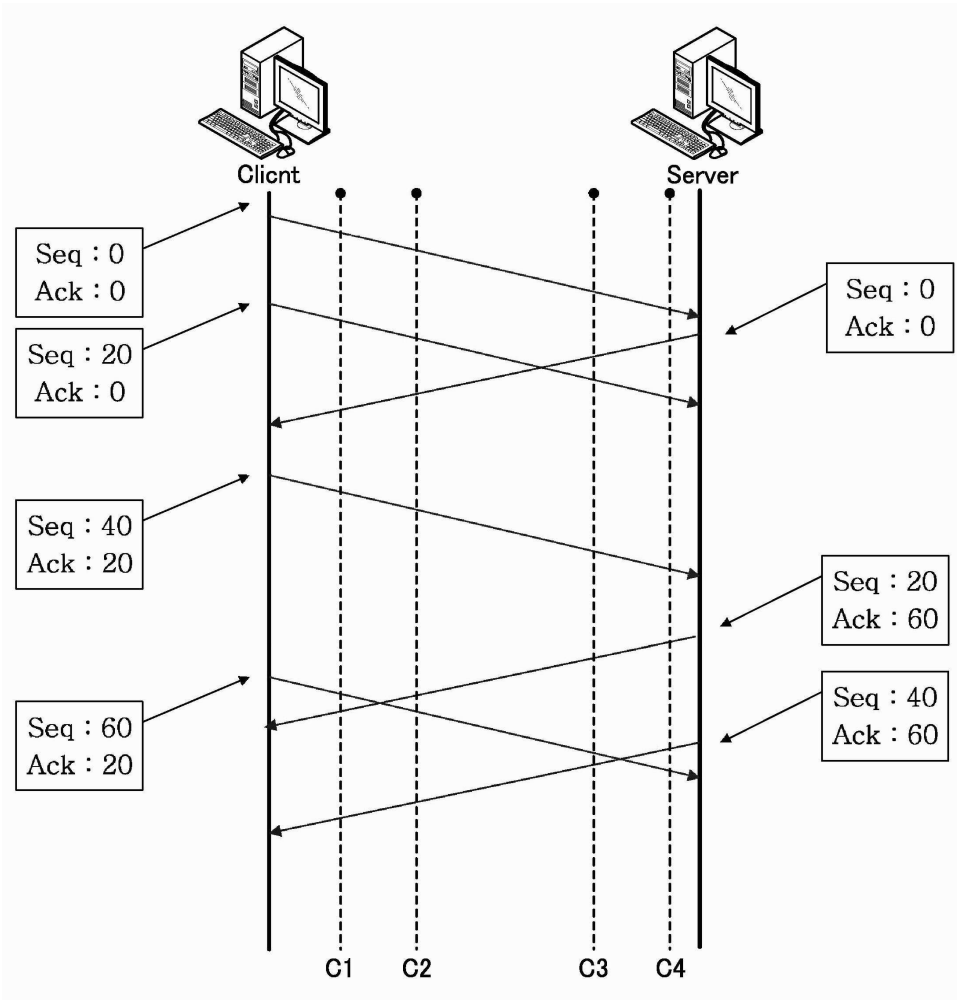
300: 비정상 순서 해결부

도면

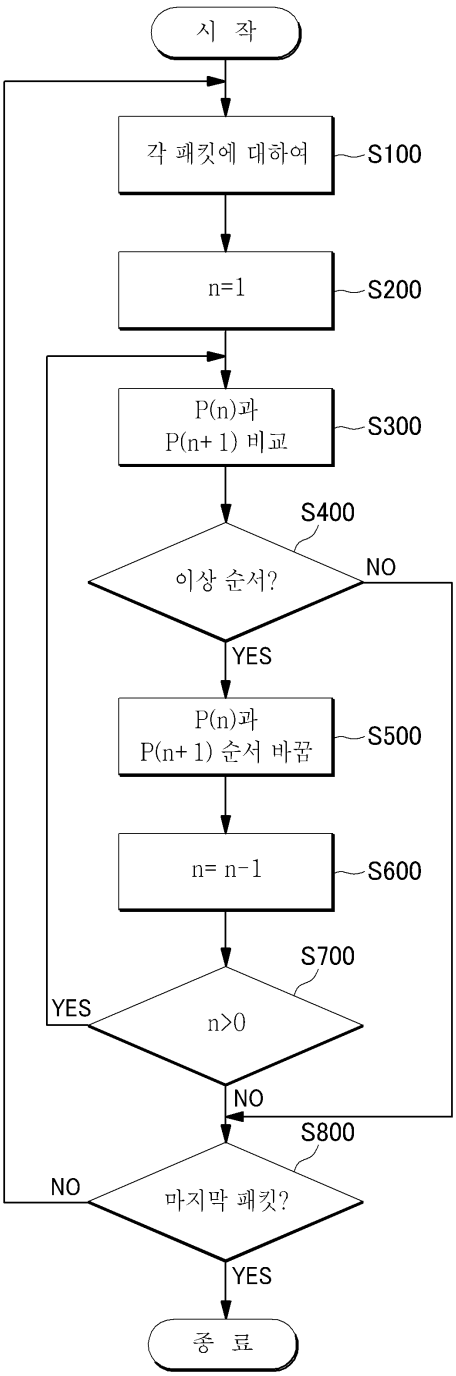
도면1


트래픽 분석 장치
10
100
트래픽 분석부
500
플로우 저장소
200
이상 순서
탐지부
400
주메모리
300
이상 순서
해결부
네 트 워 크

도면2


Clicnt
Server
Seq : 0
Ack : 0
Seq : 20
Ack : 0
Seq : 40
Ack : 20
Seq : 60
Ack : 20
Seq : 0
Ack : 0
Seq : 20
Ack : 60
Seq : 40
Ack : 60
C1
C2
C3
C4

도면3


시 작
각 패킷에 대하여
S100
n=1
S200
P(n)과
P(n+1) 비교
S300
S400
이상 순서?
NO
YES
P(n)과
P(n+1) 순서 바꿈
S500
n= n-1
S600
S700
n>0
YES
NO
S800
마지막 패킷?
NO
YES
종 료

도면4

Resolve retransmission and out-of-order problem
Remove all non-payload packets from the packet sequence

```
1: procedure Detect Normal Packet Sequence
2:       Input : packet sequence of a TCP flow
3:       if ( P(n) (direction) == P(n+1) (direction) ) then normal
4:       if ( P(n) == Fp && P(n+1) == Bp) then normal
5:       if ( P(n) == Bp && P(n+1) ==Fp) {
6:            if ( P(n)(Ack) <= P(n+1)(Seq) && P(n)(Seq) < P(n+1)(Ack) )
7:            then normal
8:            else abnormal
9:       }
10: end procedure
```

```
1: procedure Detect abnormal Packet Sequence
2:       Input : packet sequence of a TCP flow
3:       if ( P(n) ==Bp && P(n+1) ==Fp ) {
4:          if ( P(n)(Ack) <= P(n+1)(Seq) && P(n)(Seq) >= P(n+1)(Ack) ) }
5:          then abnormal
6:          else normal
7:       }
8: end procedure
```

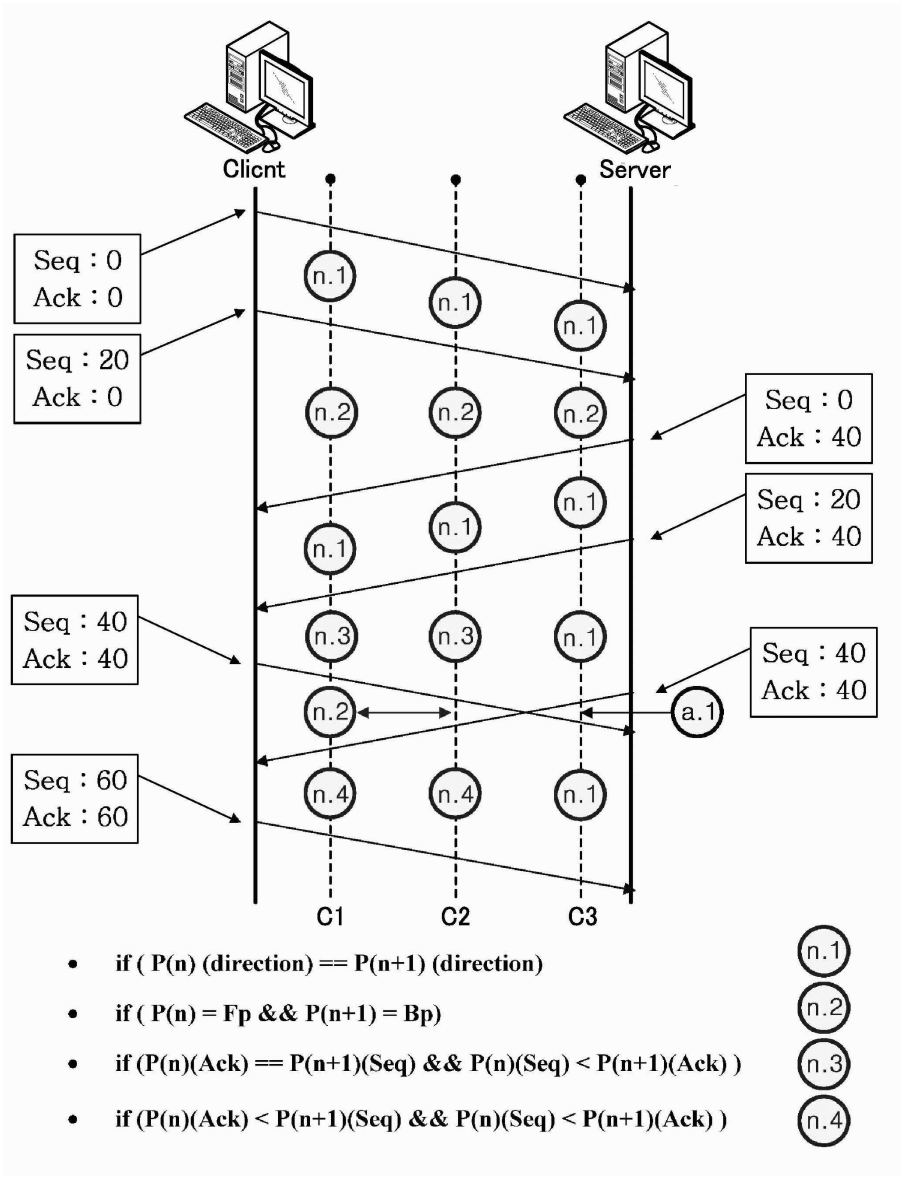
Payload packet : a packet with payload data
Non-Payload packet : a packet without payload data
P(n): n-th payload packet in a TCP flow
Forward packet (Fp) : a packet going from client to server
Backward packet (Bp) : a packet going server to client

도면5

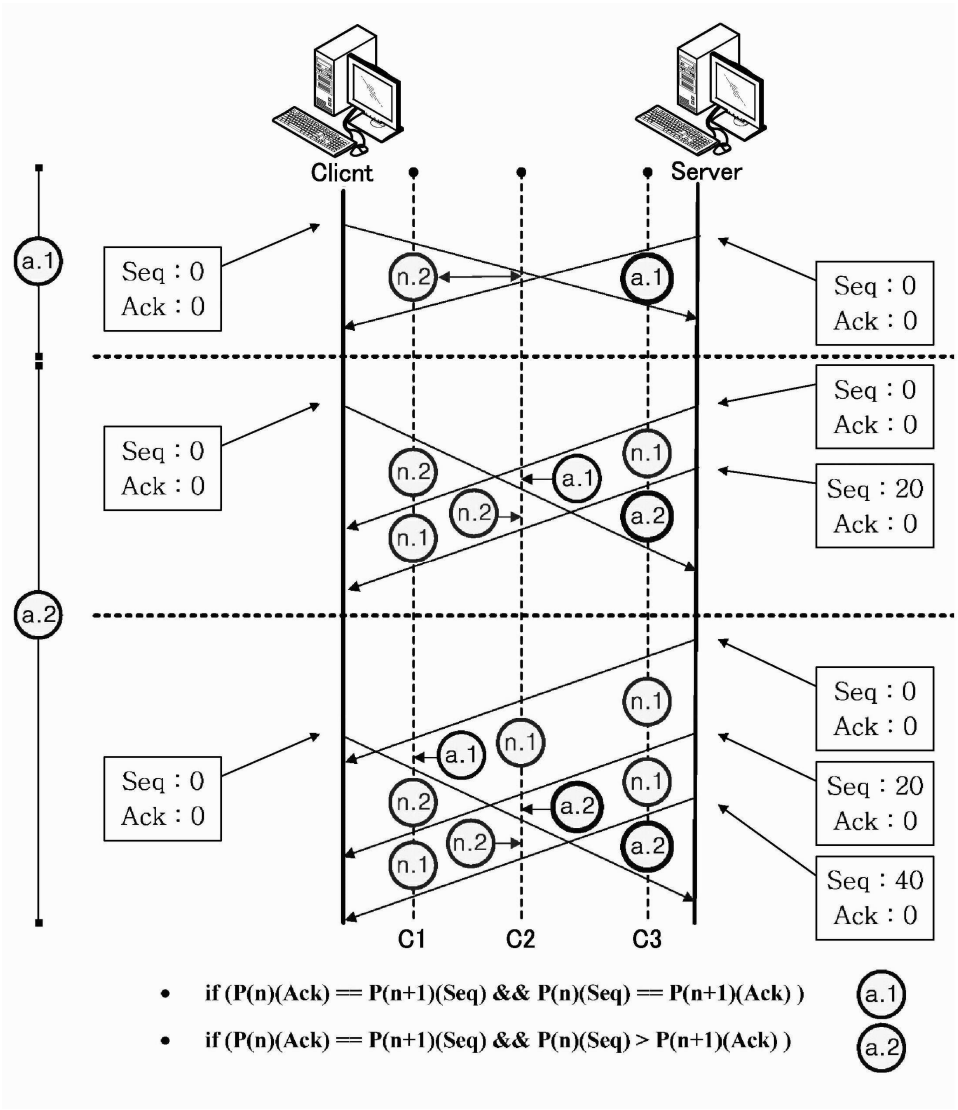
Resolve retransmission and out-of-order problem
Remove all non-payload packets from the packet

```
1: procedure Resolve Abnormal Packet Sequence
2:       Input : packet sequence of a TCP flow
3:       if ( P(n) and P(n+1) are abnormal sequence ) {
4:            change P(n) and P(n +1);
5:            n = n - 1;
6:                 if ( P(n) and P(n+1) are abnormal
7:       }
8: end procedure
```

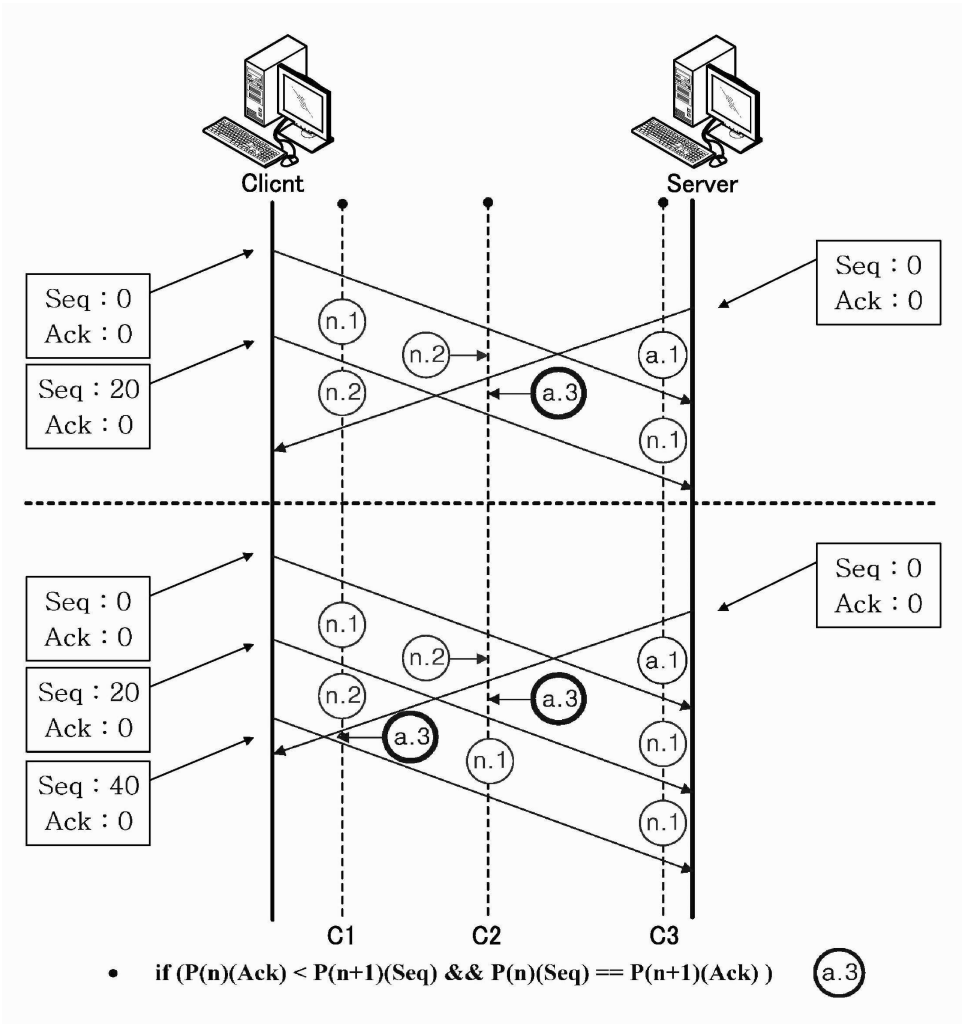
도면6


Clicnt
Server
Seq : 0
Ack : 0
Seq : 20
Ack : 0
Seq : 0
Ack : 40
Seq : 20
Ack : 40
Seq : 40
Ack : 40
Seq : 40
Ack : 40
Seq : 60
Ack : 60
n.1
n.2
n.3
n.4
a.1
C1
C2
C3
if (P(n) (direction) == P(n+1) (direction)
if (P(n) = Fp && P(n+1) = Bp)
if (P(n)(Ack) == P(n+1)(Seq) && P(n)(Seq) < P(n+1)(Ack))
if (P(n)(Ack) < P(n+1)(Seq) && P(n)(Seq) < P(n+1)(Ack))

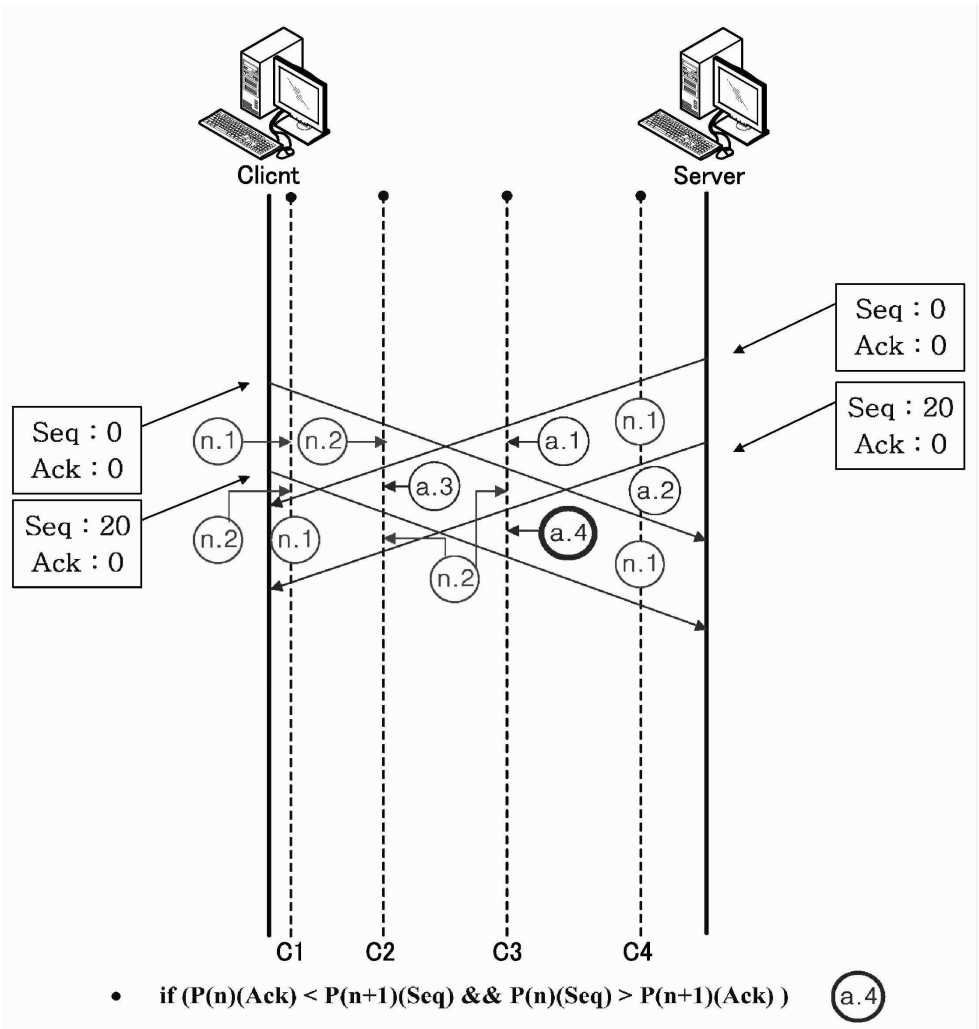
도면7


Clicnt
Server
a.1
Seq : 0
Ack : 0
n.2
a.1
Seq : 0
Ack : 0
Seq : 0
Ack : 0
Seq : 0
Ack : 0
n.2
a.1
n.1
n.2
a.2
n.1
Seq : 20
Ack : 0
a.2
Seq : 0
Ack : 0
n.1
a.1
n.1
Seq : 0
Ack : 0
n.1
n.2
a.2
Seq : 20
Ack : 0
n.2
a.2
n.1
Seq : 40
Ack : 0
C1
C2
C3
if (P(n)(Ack) == P(n+1)(Seq) && P(n)(Seq) == P(n+1)(Ack))
if (P(n)(Ack) == P(n+1)(Seq) && P(n)(Seq) > P(n+1)(Ack))
a.1
a.2

도면8


Clicnt
Server
Seq : 0
Ack : 0
Seq : 20
Ack : 0
Seq : 0
Ack : 0
n.1
n.2
n.2
a.1
a.3
n.1
Seq : 0
Ack : 0
Seq : 0
Ack : 0
Seq : 20
Ack : 0
Seq : 40
Ack : 0
n.1
n.2
n.2
a.3
a.3
n.1
a.1
a.3
n.1
n.1
C1
C2
C3
if (P(n)(Ack) < P(n+1)(Seq) && P(n)(Seq) == P(n+1)(Ack))
a.3

도면9


Clicnt
Server
Seq : 0
Ack : 0
Seq : 20
Ack : 0
Seq : 0
Ack : 0
Seq : 20
Ack : 0
n.1
n.2
a.1
n.1
a.3
a.2
n.2
n.1
a.4
n.2
n.1
C1
C2
C3
C4
if (P(n)(Ack) < P(n+1)(Seq) && P(n)(Seq) > P(n+1)(Ack))
a.4