

	(19) 대한민국특허청(KR) (12) 공개특허공보(A)	(11) 공개번호 10-2013-0142489 (43) 공개일자 2013년12월30일
(51) 국제특허분류(Int. Cl.) H04L 29/08 (2006.01)	(71) 출원인 충남대학교산학협력단	
(21) 출원번호 10-2012-0065745	대전광역시 유성구 대학로 99 (궁동, 충남대학교)	
(22) 출원일자 2012년06월19일	(72) 발명자	
심사청구일자 2012년06월19일	이연희	
	대전광역시 유성구 노은로 353 송림마을아파트 304동 1701호	
	이영석	
	대전광역시 유성구 테크노중앙로 32 금성백조아파트 809-602 (관평동)	
	(74) 대리인	
	김원준	

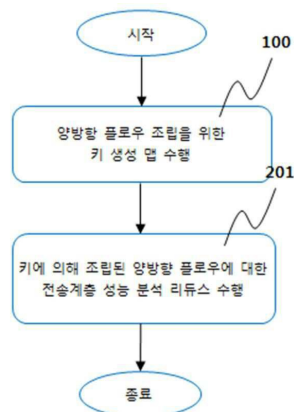
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 맵리듀스 방식을 이용한 전송계층의 성능 분석 방법

(57) 요약

본 발명은 맵리듀스 방식을 기반으로 네트워크 상에서 수집되는 대량의 트래픽으로부터 전송계층의 성능을 효율적으로 분석할 수 있는 방법에 관한 것으로, 보다 상세하게는 (a) 트래픽에 대한 패킷 트레이스 파일로부터 양방향 플로우를 조립하기 위한 키를 생성하여 레코드를 출력하는 맵 단계; (b) 상기 출력된 레코드에 대해 상기 키 값로부터 양방향 플로우를 조립하고 전송계층 성능 분석을 수행하는 리듀스 단계;를 포함하는 것을 특징으로 하는 네트워크 전송계층의 성능 분석 방법에 관한 것이다.

대표도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호 08913-05002

부처명 방송통신위원회

연구사업명 방송통신 기술개발 사업

연구과제명 초정밀 측정 및 분석 기술 연구

기 여 율 1/1

주관기관 KAIST

연구기간 2012.03.01 ~ 2013.02.28

특허청구의 범위

청구항 1

- (a) 트래픽에 대한 패킷 트레이스 파일로부터 양방향 플로우를 조립하기 위한 키를 생성하여 레코드를 출력하는 맵 단계;
- (b) 상기 출력된 레코드에 대해 상기 키 값로부터 양방향 플로우를 조립하고 전송계층 성능 분석을 수행하는 리듀스 단계;
- 를 포함하는 것을 특징으로 하는 네트워크 전송계층의 성능 분석 방법.

청구항 2

제 1 항에 있어서,
상기 키는 클라이언트(client) IP 주소, 클라이언트 포트(port) 번호, 서버(server) IP 주소, 서버 포트 번호 및 프로토콜의 조합에 의해 형성된 클라이언트-서버 키인 것을 특징으로 하는 네트워크 전송계층의 성능 분석 방법.

청구항 3

제 2 항에 있어서,
상기 클라이언트와 상기 서버는,
두 호스트 간의 세션을 맺기 위해 두 호스트 간에 주고 받는 패킷으로부터 SYN 플래그와 SYN에 대한 ACK 플래그를 가지는 패킷을 식별하고,
최초에 SYN을 요청한 호스트를 클라이언트로,
SYN에 대한 ACK를 전송한 호스트를 서버로 식별하는 것을 특징으로 하는 네트워크 전송계층의 성능 분석 방법.

청구항 4

제 2 항에 있어서,
상기 클라이언트와 상기 서버는,
두 호스트 간에 주고 받는 패킷으로부터 두 호스트 중 최초에 패킷을 전송한 쪽을 클라이언트로,
다른 한 쪽은 서버로 식별하는 것을 특징으로 하는 네트워크 전송계층의 성능 분석 방법.

청구항 5

제 1 항 또는 제 2 항에 있어서,
상기 양방향 플로우는 패킷에서 FIN이나 RESET 플래그를 인지하여 하나의 세션이 종료되는 것을 식별하는 것을 특징으로 하는 네트워크 전송계층의 성능 분석 방법.

청구항 6

제 1 항 또는 제 2 항에 있어서,

상기 양방향 플로우를 패킷의 시간 간격을 확인하여 통상 하나의 플로우라고 인식할 수 있는 시간 간격의 제한 값을 넘는 경우 서로 다른 플로우로 식별하는 것을 특징으로 하는 네트워크 전송계층의 성능 분석 방법.

청구항 7

제 2 항에 있어서,

플로우에 SYN 플래그와 SYN에 대한 ACK 플래그를 갖는 패킷이 존재하지 않는 경우,

상기 맵단계는 출발지(source) IP를 클라이언트로, 도착지(destination) IP를 서버로 정의하여 클라이언트-서버 키를 생성하여 리듀서에 전달하는 동시에, 도착지 IP를 클라이언트로 출발지 IP를 서버로 정의하여 클라이언트-서버 키를 생성하여 레코드를 출력하고;

상기 리듀스단계는 출력된 레코드에 대해 상기 키 값로부터 양방향 플로우를 조립하고, 상기 양방향 플로우에서 SYN 플래그와 SYN에 대한 ACK 플래그를 갖는 패킷이 존재하는 플로우에 대해서만 전송계층의 성능 분석을 수행하는 것을 특징으로 하는 네트워크 전송계층의 성능 분석 방법.

청구항 8

제 1 항에 있어서,

네트워크 서버넷의 주소를 알고 있을 경우,

상기 키는 모니터링할 플로우를 공유하는 두 호스트가 서버넷 내에 존재하는 내부 호스트인지 외부에 존재하는 외부 호스트인지 식별하는 것에 의해 생성된 내부-외부 호스트 키인 것을 특징으로 하는 네트워크 전송계층의 성능 분석 방법.

청구항 9

제 1 항 또는 제 2 항 또는 제 8 항에 있어서,

상기 맵단계는 하나의 패킷에 대해 (a) 요청 패킷;과 (b)요청 패킷에 대한 응답으로서의 패킷;에 대한 레코드를 생성하는 것을 특징으로 하는 네트워크 전송계층의 성능 분석 방법.

청구항 10

제 9 항에 있어서,

상기 요청 패킷에 대한 레코드는 sequence 번호에 페이로드의 길이를 더하여 응답 패킷의 ACK 번호와 동일한 값을 키로 추가하여 생성하고,

상기 응답 패킷으로서의 레코드는 ACK 번호를 키로 추가하여 생성하는 것을 특징으로 하는 네트워크 전송계층의 성능 분석 방법.

명세서

기술분야

본 발명은 전송계층의 성능 분석 방법에 관한 것으로, 맵리듀스 방식을 기반으로 네트워크 상에서 수집되는 대량의 트래픽으로부터 전송계층의 성능을 효율적으로 분석할 수 있는 방법에 관한 것이다.

배경기술

[0001]

- [0002] 네트워크에서 데이터가 전송되는 양의 정도를 나타내는 네트워크 트래픽을 측정·분석하는 일은 컴퓨터 네트워크 분야를 연구하는데 있어서 기본적으로면서도 가장 중요한 분야 중 하나이다. 전송계층(Transport layer)은 계층 구조의 네트워크 구성요소와 프로토콜 내에서 송신자와 수신자를 연결하는 통신 서비스를 제공한다. 전송 프로토콜 중 가장 잘 알려진 것은 연결지향 전송방식을 사용하는 TCP(Transmission Control Protocol, 전송 제어 프로토콜)이며, UDP(User Datagram Protocol, 사용자 데이터그램 프로토콜)는 보다 단순한 전송에 사용된다. 인터넷을 이용하는 대부분의 응용들은 전송계층 위에서 동작한다. 따라서 이런 응용계층의 서비스의 질은 TCP나 UDP와 같은 전송계층의 성능에 따라 판가름 지어진다고 할 수 있다. 트래픽의 측정은 네트워크의 운영 상태와 안정성, 그리고 트래픽 특성 파악, 설계 및 계획, 유해한 트래픽의 차단, 과금, QoS(Quality of Service) 보장을 위해 필수적이다.
- [0003] 전송계층의 대표적인 성능 측정 메트릭으로는 RTT(Round-Trip time), CWnd(혼잡 윈도우: Congestion Window), 처리량(Throughput), 재전송율 등이 있다. 이러한 메트릭을 측정하기 위해서는 두 호스트 간에 주고 받은 요청(REQ)과 응답(ACK)을 담은 양쪽 방향의 트래픽이 모두 필요하다. 즉 클라이언트로부터 서버로의 트래픽과 서버에서 클라이언트로의 트래픽이 있어야 두 호스트 간의 전송계층의 성능을 계산할 수 있다.
- [0004] 하지만 대량으로 수집되는 인터넷 트래픽에 대해, 상기와 같은 성능 메트릭을 계산하기 위해서는 지속적으로 유입되는 트래픽의 저장과 처리가 뒷받침되어야 하므로 이를 지원하기 위한 높은 컴퓨팅 자원과 저장공간을 가지는 고가의 장비가 요구된다. 또한 인터넷 트래픽의 규모가 더욱 성장함에 따라 주기적으로 더 향상된 고가의 장비로 교체하여야 하므로 상당한 비용의 발생을 초래한다. 따라서, 현재와 같이 날로 증가하는 트래픽에 대해 안정적으로 성능을 분석하는 일은 점점 더 어려운 일이 되고 있다.
- [0005] 맵리듀스(MapReduce)은 대용량의 데이터를 안정적으로 처리하기 위한 프로그래밍 모델로서 구글(Google)에 의해 제안되었다. 이 방식을 이용하면 저가의 컴퓨팅 장비를 이용한 분산 프로그래밍이 가능하며, 이러한 맵리듀스를 오픈소스로 구현한 것이 바로 하둡(Hadoop)이다.
- [0006] 맵리듀스는 맵과 리듀스 단계의 처리과정을 통해 대량의 데이터를 처리하는 방식으로 각 단계는 입력과 출력으로 키와 값의 쌍을 가진다. 맵 단계에서는 주로 대량의 데이터로부터 유입되는 레코드 형태의 Key-Value의 쌍으로부터 처리하려고 하는 Key에 해당하는 값과 Value에 해당하는 값을 추출하는 일을 수행한다. 리듀스 단계에서는 맵 단계에서 추출한 Key에 그룹핑되어 전달되는 일련의 Value들을 순회하며 원하는 계산을 수행하여 결과를 얻어내는 일을 수행한다. 따라서, 사용자는 자신의 목적에 적합하게 맵 함수와 리듀스 함수를 정의하면, 하나의 클러스터 안에 있는 분산된 컴퓨팅 자원을 이용하여 대용량의 데이터를 분산 및 병렬 처리할 수 있다.
- [0007] 맵리듀스를 이용한 대용량 데이터의 처리는 대용량 웹 문서에서 특정 단어가 포함된 라인의 추출, 특정 URL이 포함된 개수를 비롯하여 다양한 분야에서 데이터의 분산 처리에 사용되고 있으나, 이를 이용한 전송계층의 성능 분석 방법에 대해서는 아직 개발된 바 없다.

발명의 내용

해결하려는 과제

- [0008] 상기와 같은 종래기술의 문제점을 해소하기 위한 본 발명의 목적은 맵리듀스 방식을 이용하여 다수의 서버에서 두 호스트 간에 주고 받은 요청과 응답을 담은 양방향 트래픽을 조립하여 분산 분석하여 효율적으로 전송계층의 성능을 분석할 수 있는 병렬 처리 방법을 제공하는 것이다.

과제의 해결 수단

- [0009] 전술한 목적을 달성하기 위한 본 발명은 (a) 트래픽에 대한 패킷 트레이스 파일로부터 양방향 플로우를 조립하기 위한 키를 생성하여 레코드를 출력하는 맵 단계; (b) 상기 출력된 레코드에 대해 상기 키 값로부터 양방향 플로우를 조립하고 전송계층 성능 분석을 수행하는 리듀스 단계;를 포함하는 것을 특징으로 하는 네트워크 전송계층의 성능 분석 방법에 관한 것이다.
- [0010] 대량의 트래픽에 대해 하나 이상의 패킷 트레이스 파일이 여러 개의 블록으로 분산되어 저장되는 하둡과 같은

분산 시스템에서 네트워크의 전송계층의 성능을 분석하기 위해서, 상기 키는 클라이언트(client) IP 주소, 클라이언트 포트(port) 번호, 서버(server) IP 주소, 서버 포트 번호 및 프로토콜의 조합에 의해 형성된 클라이언트-서버 키인 것이 바람직하다.

[0011] 만일 네트워크 서버넷의 주소를 알고 있을 경우, 상기 키로 모니터링할 플로우를 공유하는 두 호스트가 서버넷 내에 존재하는 내부 호스트인지 외부에 존재하는 외부 호스트인지 식별하는 것에 의해 생성된 내부-외부 호스트 키를 사용할 수 있다.

발명의 효과

[0012] 이상과 같이 본 발명에 의하면, 저가의 컴퓨터를 이용하여 대량의 인터넷 트래픽 데이터를 맵리듀스 방식을 이용하여 전송계층의 성능 측정을 여러 대의 컴퓨팅 노드에 분산하여 측정할 수 있다. 특히 전송계층의 성능 분석은 두 호스트 간의 양 방향 플로우로부터 요청과 요청에 대한 응답을 감지하여 계산되는 특성이 있는데 본 발명의 방법에 의하면 여러 대의 노드가 맵리듀스 방식을 이용하여 효율적으로 데이터를 분배하여 처리할 수 있다.

도면의 간단한 설명

[0013] 도 1은 맵리듀스 기반의 전송계층의 성능 분석을 위한 흐름도.

도 2은 맵리듀스 기반의 전송계층 성능 분석을 위한 한 개 이상에 분산된 양방향 플로우의 조립 방법의 흐름도.

도 3는 두 개 이상의 블록에 놓여 있는 플로우를 재조립하기 위한 방법의 흐름도.

도 4은 맵리듀스 기반의 양방향 플로우 조립을 통한 네트워크 전송계층 성능분석 흐름도.

발명을 실시하기 위한 구체적인 내용

[0014] 이하 첨부된 도면을 참조하여 본 발명을 보다 상세히 설명한다. 그러나 이러한 도면은 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.

[0015] 도 1는 본 발명에 의한 맵리듀스를 기반으로 한 전송계층의 성능분석을 위한 흐름도이다. 전송계층의 성능을 분석하기 위해서는 두 호스트 간에 주고 받은 요청과 응답을 담은 양쪽 방향의 트래픽이 모두 필요하다. 따라서, 먼저 트래픽에 대한 패킷 트레이스 파일로부터 양방향 플로우의 조립을 위한 키를 생성하는 맵 작업을 수행한다(100). 이후 리듀스 작업에 의해 맵의 결과로서 생성된 키에 의해 양방향 플로우를 조립하여 전송계층의 성능 분석(200)을 수행한다.

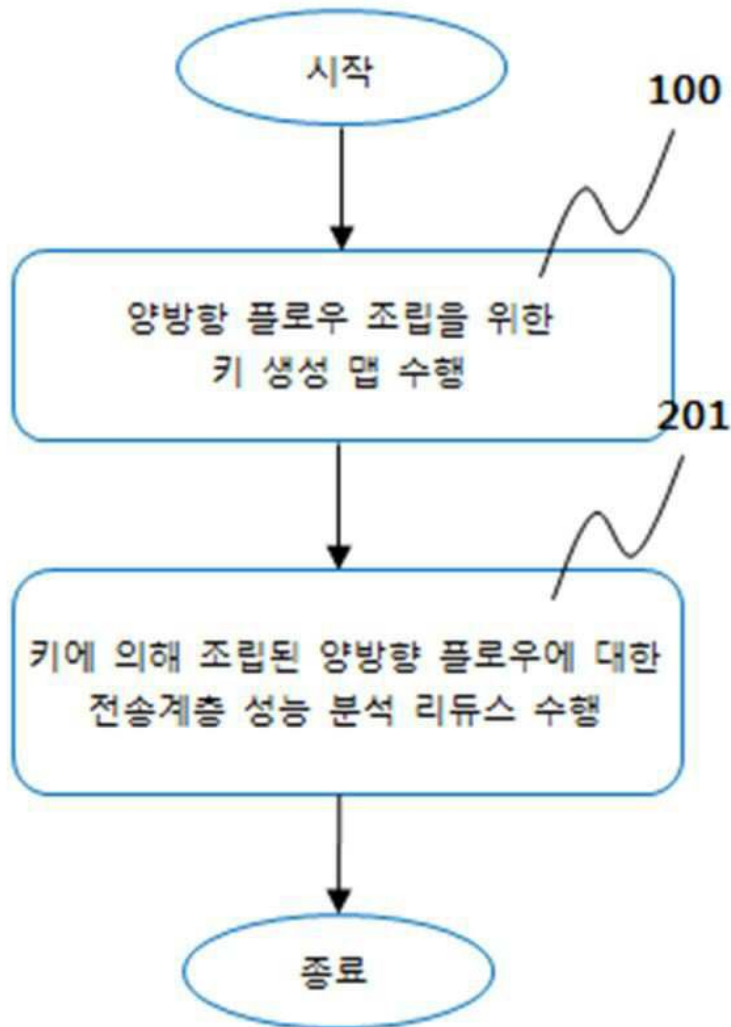
[0016] 대량의 트래픽에 대해 하나 이상의 패킷 트레이스 파일이 여러 개의 블록으로 분산되어 저장되는 하둡과 같은 분산 시스템에서는, 네트워크의 전송계층의 성능을 분석하기 위해서는 두 호스트 간의 요청과 응답에 해당하는 플로우를 그루핑하여 하나의 리듀서에서 분석할 수 있도록 하여야 한다. 도 2는 본 발명에 의해 하나 이상의 블록에 분산되어 저장된 양방향 플로우를 조립하는 방법을 나타낸다. ①은 통상적으로 플로우를 식별하기 위해 사용하는 5튜플 값인 source IP, source port, destination IP, destination port, protocol을 조합하여 출발지-도착지 키로 생성하여 사용할 경우의 리듀서의 할당을 나타낸다. 5튜플 키 값을 출발지-도착지 키로 생성하여 사용하는 경우, 클라이언트로부터 서버로의 플로우(C2S flow)와 서버로부터 클라이언트로의 플로우(S2C flow)가 다른 해시값을 가지므로 다른 리듀서에 할당될 가능성이 많으므로 리듀서에서 양방향 플로우를 가지고 성능 분석을 할 수 없게 된다. 반면, ②와 같이 두 호스트에 대해 클라이언트와 서버를 식별하여 client IP, client port, server IP, server port, protocol 값을 조합한 클라이언트-서비 키를 사용한다면, 클라이언트에서 서버로의 플로우와 서버로부터 클라이언트로의 플로우가 같은 키의 해시값을 가지게 하므로서 같은 리듀서에 할당되도록 할 수 있으므로 양방향 플로우에 대해 전송계층의 성능을 분석하는 것이 가능하게 된다.

- [0017] TCP의 경우, 두 호스트 간의 세션을 맺기 위해 두 호스트 간에 주고 받는 패킷으로부터 SYN 플래그와 SYN에 대한 ACK 플래그를 갖는 패킷을 식별하여, 최초로 SYN을 요청한 호스트를 클라이언트로, SYN에 대한 ACK를 전송한 쪽을 서버로 하여 클라이언트와 서버를 식별할 수 있다. UDP의 경우 프로토콜의 특성 상 두 호스트 간의 세션을 맺기 위한 SYN과 SYN에 대한 ACK의 과정이 존재하지 않으므로 상기 방법을 적용할 수 없다. 따라서 UDP의 경우 두 호스트 중 최초로 패킷을 전송한 쪽을 클라이언트로 반대쪽을 서버로 식별하는 것으로 대체가 가능하다. 또한 UDP를 사용하는 상위의 응용계층에서 플로우 내의 일련번호와 타임스탬프 같은 기능을 하는 필드를 인식하여 클라이언트와 서버를 식별하는데 사용하는 것도 가능하다.
- [0018] 식별된 두 호스트, 즉 클라이언트와 서버 간에 여러 번의 플로우가 존재할 경우, 하나의 양방향 플로우를 식별하기 위한 방법으로 TCP의 경우에는 패킷에서 FIN이나 RESET 플래그를 인지하여 하나의 세션이 종료됨을 식별하는 것이 가능하다. UDP의 경우에는 명시적인 종료 플래그가 존재하지 않으므로 두 호스트 간에 주고 받은 패킷의 시간 간격을 확인하여 통상 하나의 플로우라고 인식할 수 있는 시간 간격의 제한 값을 넘는 경우 서로 다른 플로우로 식별하는 방법이 가능하다. 통상, 하나의 플로우라고 인식할 수 있는 패킷의 도착 시간 간격은 응용계층의 특성에 따라 정의되어야 하지만 CISCO에서 정의한 NetFlow의 경우 기본 30분을 사용하며 1분에서 60분 사이의 값으로 정의하도록 한다. 예를 들면 두 호스트 간 30분 이상 패킷 전달이 없었다면 하나의 세션이 종료된 것으로 식별할 수 있다. 이 방법은 네트워크 상에 에러나 고의적인 의도에 의해 TCP에서 명시적인 세션 종료 플래그가 누락되었을 경우에도 적용이 가능하다.
- [0019] 하나 이상의 패킷 트레이스 파일이 여러 개의 블록으로 분산되어 저장되는 분산 시스템에서 하나의 양방향 플로우가 두 개 이상의 블록에 걸쳐 놓여있다면, 플로우의 후반부를 가진 블록을 처리하는 매퍼의 경우 플로우 내에 세션을 맺기위한 SYN, SYN+ACK 패킷이 존재하지 않기 때문에 클라이언트-서버 키를 생성할 수 없다.
- [0020] 도 3은 두 개 이상의 블록에 걸쳐 놓여 있는 하나의 양방향 플로우를 재조립하기 위한 방법을 나타내는 흐름도이다. 도 3에서 ③번 플로우의 전반부는 블록 1에 플로우의 후반부는 블록 2에 분산되어 저장되어 있다. 블록 2에 있는 ③번 플로우의 후반부는 SYN이나 SYN에 대한 ACK가 블록 1에 존재하므로 이들 패킷만으로는 두 호스트에 대한 클라이언트와 서버를 식별할 수 없다. 이렇게 패킷에 SYN 플래그와 SYN에 대한 ACK 플래그가 누락되어 있는 경우에는 source IP를 클라이언트로, destination IP를 서버로 정의하여 클라이언트-서버 키를 생성하여 리듀서에 전달하는 동시에, destination IP를 클라이언트로 source IP를 서버로 정의하여 클라이언트-서버 키를 생성하여 리듀서에 전달한다. 이후 리듀서에서는 맵의 결과로서 키에 의해 조립된 양방향 플로우에 대해 SYN 플래그와 SYN에 대한 ACK 플래그의 유무를 판단하여 블록 1에서와 같이 세션 초기화 메시지가 존재하는 플로우에 대해서는 전송계층의 성능 분석을 실시하고, 블록 2와 같이 세션 초기화가 존재하지 않은 플로우의 경우 일련의 패킷을 버리는 것에 의해 분산 시스템에서의 전송계층의 성능 분석이 가능하다.
- [0021] 만일 이미 분석해야할 네트워크 서버넷의 주소를 알고 있다면, 전술한 세션의 초기화 메시지를 통해서 클라이언트와 서버를 식별하여 키를 생성하는 대신, 모니터링할 서버넷 내에 존재하는 내부 호스트인지 외부에 존재하는 호스트인지를 식별하고 내부-외부 호스트 키를 생성하여 리듀서에 전달하는 방법으로 플로우를 조립하여 전송계층의 성능을 분석할 수 있다.
- [0022] 전송계층의 성능 측정은 종래의 성능 메트릭으로 알려진 RTT(Round-Trip time), CWnd(혼잡 윈도우: Congestion Window), 처리량(Throughput), 재전송 등을 측정하는 것에 의해 이루어질 수 있다. 예를 들어, RTT의 경우 요청 패킷이 송신한 시간에 대한 응답패킷의 도착 시간의 차이를 계산하여 측정할 수 있다. 재전송(RTX)의 경우에도 요청 패킷에 대한 동일한 패킷을 요청하는 응답 패킷의 수를 측정하여 재전송 수나 재전송의 원인 측정이 가능하다. 전술한 본 발명의 방법에 따라 리듀스 작업에 의해 맵의 결과로서 키에 의해 조립된 양방향 플로우에 대해 전송계층의 성능 분석을 수행하는 경우, 플로우 내에서 요청 패킷과 응답 패킷을 찾아서 순회하여야 하므로 분석 성능의 저하를 초래할 수 있다. 이러한 문제를 해결하기 위하여, 도 4에 도시된 바와 같이 매퍼에서 하나의 패킷에 대해 요청 패킷과 요청 패킷에 대한 응답으로서의 패킷 두 개를 생성하여 리듀서에 전달하는 것이 바람직하다.
- [0023] 요청 패킷과 요청에 대한 응답 패킷이 하나의 그룹으로 전달되게 하기 위해서는 TCP 요청 패킷으로서의 레코드 생성 시에는 sequence 번호에 패이로드의 길이를 더하여 응답 패킷의 ack 번호와 동일한 값을 가지는 키로 추가

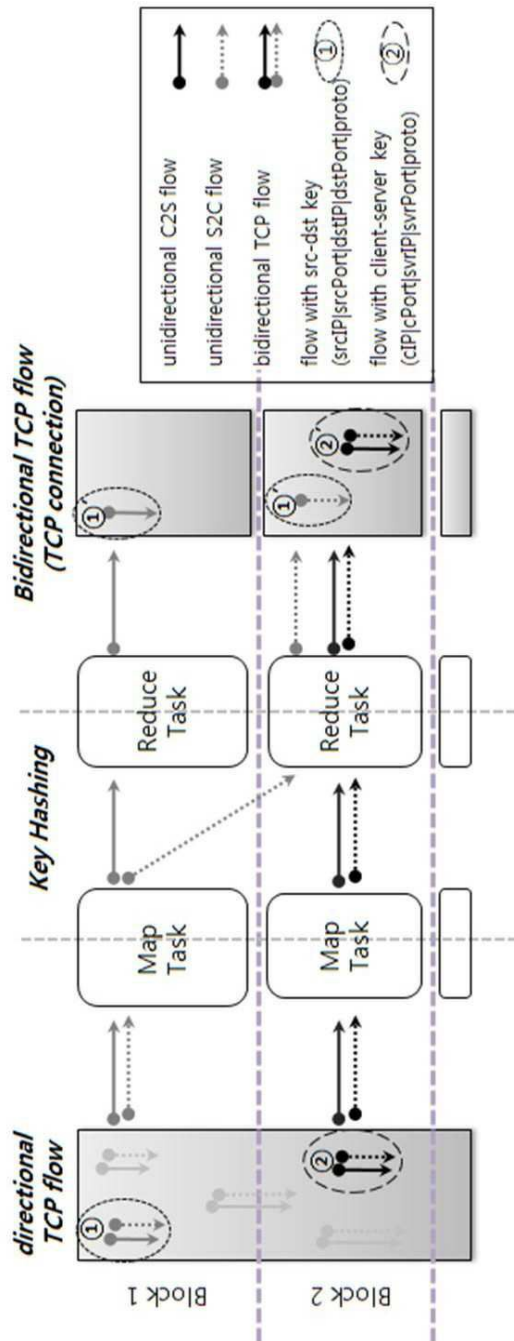
하여 리듀서에 전달하고 응답(ACK) 패킷으로서의 레코드 생성 시에는 ack 번호를 키로 추가함으로써 요청 패킷과 응답패킷이 같은 키를 공유하여 그루핑되게 하는 방법으로 처리가 가능하다. 상기에서 제시한 구체적인 키 값은 사용하는 TCP의 종류와 버전에 따라 변경하여 적용할 수 있다.

도면

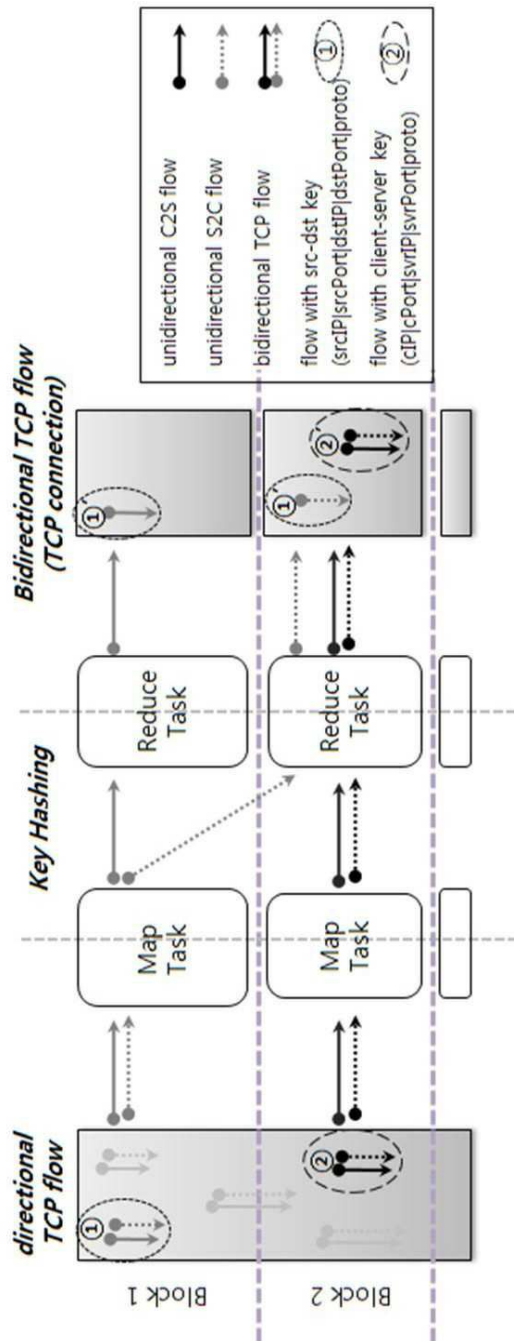
도면1



도면2



도면3



도면4

