(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0079088
(43) 공개일자 2017년07월10일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/085 (2013.01)
H04L 9/0819 (2013.01)
(21) 출원번호 10-2015-0189270
(22) 출원일자 2015년12월30일
심사청구일자 2015년12월30일

(71) 출원인
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
(72) 발명자
리시
서울시 서대문구 이화여대7길 46,4층 영재리빙텔 207호 (대현동)
채기준
서울특별시 강남구 강남대로136길 34
도인실
인천광역시 연수구 센트럴로 194, 201동 2705호(송도동, 더샵 센트럴파크2)
(74) 대리인
특허법인(유한)아이시스

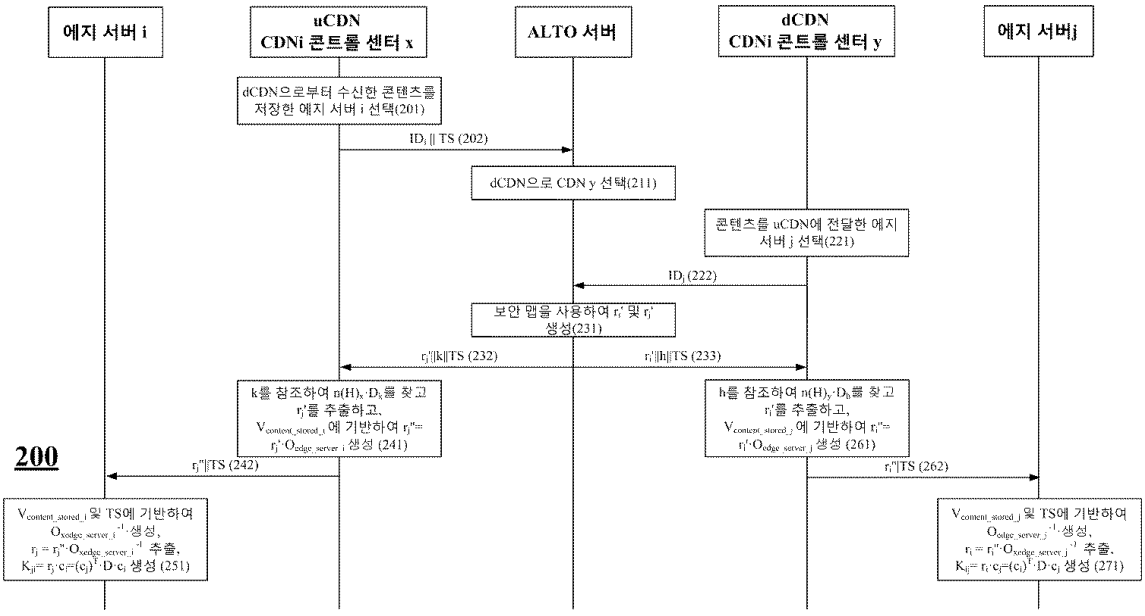
전체 청구항 수 : 총 6 항

(54) 발명의 명칭 **CDNi에서 CDN 사이에 암호화를 위한 키를 공유하는 방법**

(57) 요 약

CDNi에서 CDN 사이에 암호화를 위한 키를 공유하는 방법은 CDNi를 구성하는 복수의 CDN에 각각 속한 에지 서버가 λ 크기의 열 벡터를 생성하는 단계, ALTO 서버가 상기 열 벡터 및 λ×λ 크기의 대칭 행렬의 집합 D'를 저장하는 단계, 상기 ALTO 서버는 uCDN의 에지 서버 i의 열 백터를 이용하여 블롬 기법에서 사용하는 제1 행 벡터 r_j를 생성하고, dCDN의 에지 서버 j에 대한 열 벡터를 이용하여 블롬 기법에서 사용하는 제2 행 벡터 r_i를 생성하는 단계, 상기 ALTO 서버는 상기 행 벡터 r_j를 상기 에지 서버 i에 전달하고, 상기 행 벡터 r_i를 상기 에지 서버 j에 전달하는 단계 및 상기 에지 서버 i는 자신이 생성한 열 백터와 상기 제1 행 벡터를 곱하여 제1 키를 생성하고, 상기 에지 서버 j는 자신이 생성한 열 벡터와 상기 제2 행 벡터를 곱하여 제2 키를 생성하는 단계를 포함한다.

대 표 도



(52) CPC특허분류
H04L 9/0838 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 2013R1A1A2011788
부처명 교육부
연구관리전문기관 한국연구재단
연구사업명 기초연구사업(학술진흥)
연구과제명 CDNi 환경에서의 안전하고 효율적인 서비스보안 기법
기 여 율 1/1
주관기관 이화여자대학교 산학협력단
연구기간 2015.06.01 ~ 2016.05.31

명 세 서

청구범위

청구항 1

CDNi를 구성하는 복수의 CDN에 각각 속한 에지 서버가 λ 크기의 열 벡터를 생성하는 단계;

ALTO 서버가 상기 열 벡터 및 λ×λ 크기의 대칭 행렬의 집합 D'를 저장하는 단계;

상기 ALTO 서버는 uCDN의 에지 서버 i의 열 벡터를 이용하여 블롬 기법에서 사용하는 제1 행 벡터 r_j를 생성하고, dCDN의 에지 서버 j에 대한 열 벡터를 이용하여 블롬 기법에서 사용하는 제2 행 벡터 r_i를 생성하는 단계;

상기 ALTO 서버는 상기 행 벡터 r_j를 상기 에지 서버 i에 전달하고, 상기 행 벡터 r_i를 상기 에지 서버 j에 전달하는 단계; 및

상기 에지 서버 i는 자신이 생성한 열 백터와 상기 제1 행 벡터를 곱하여 제1 키를 생성하고, 상기 에지 서버 j는 자신이 생성한 열 벡터와 상기 제2 행 벡터를 곱하여 제2 키를 생성하는 단계를 포함하는 CDNi에서 CDN 사이에 암호화를 위한 키를 공유하는 방법.

청구항 2

제1항에 있어서,

상기 에지 서버 j가 상기 제2 키를 사용하여 데이터를 암호화하여 상기 에지 서버 i에 전달하고, 상기 에지 서버 i는 데이터를 상기 제1 키를 사용하여 복호하는 단계를 더 포함하는 CDNi에서 CDN 사이에 암호화를 위한 키를 공유하는 방법.

청구항 3

제1항에 있어서,

상기 ALTO 서버는 상기 대칭 행렬의 집합 D'에서 어느 하나의 대칭 행렬 D를 선택하고, 상기 에지 서버 i의 열 벡터와 D를 이용하여 상기 제1 행 벡터를 생성하고, 상기 에지 서버 j의 열 벡터와 D를 이용하여 상기 제2 행 벡터를 생성하는 CDNi에서 CDN 사이에 암호화를 위한 키를 공유하는 방법.

청구항 4

제1항에 있어서,

상기 ALTO 서버는 일 방향 함수를 모든 CDN에 전달하는 단계를 더 포함하고,

상기 ALTO 서버는 상기 함수에 상기 에지 서버 i가 생성한 열 백터를 적용한 상기 제1 열 벡터를 상기 에지 서버 j에 전달하고, 상기 함수에 상기 에지 서버 j가 생성한 열 백터를 적용한 상기 제2 열 벡터를 상기 에지 서버 i에 전달하고,

상기 에지 서버 i는 상기 함수에 자신이 생성한 열 백터를 적용하여 상기 제1 열 백터를 생성하고, 상기 에지 서버 j는 상기 함수에 자신이 생성한 열 백터를 적용하여 상기 제2 열 벡터를 생성하는 CDNi에서 CDN 사이에 암호화를 위한 키를 공유하는 방법.

청구항 5

제1항에 있어서,

상기 ALTO 서버가 CDNi에 속한 CDN의 개수×λ 크기의 행렬 H를 저장하는 단계;

상기 ALTO 서버가 상기 복수의 CDN의 콘트롤 센터 각각에 대해 상기 행렬 H 중 해당 CDN에 대한 행 벡터를 전달하는 단계;

상기 ALTO 서버가 상기 행렬 H에서 상기 에지 서버 j에 대한 제3 행 벡터를 찾고, 상기 제3 행 백터를 이용하여

상기 제1 행 벡터를 암호화하여 상기 dCDN의 콘트롤 센터에 전달하고, 상기 행렬 H에서 상기 에지 서버 i에 대한 제4 행 벡터를 찾고, 상기 제4 행 벡터를 이용하여 상기 제2 행 벡터를 암호화하여 상기 uCDN의 콘트롤 센터에 전달하는 단계; 및

상기 dCDN의 콘트롤 센터는 자신이 수신한 상기 제3 행 백터를 이용하여 상기 제1 행 백터를 복호하고, 상기 uCDN의 콘트롤 센터는 자신이 수신한 상기 제4 행 벡터를 이용하여 상기 제2 행 벡터를 복호하는 단계를 더 포함하는 CDNi에서 CDN 사이에 암호화를 위한 키를 공유하는 방법.

청구항 6

제5항에 있어서,

상기 dCDN의 콘트롤 센터는 상기 제1 행 벡터를 콘텐츠 서비스 사업자의 개수의 크기를 갖는 암호화 벡터로 연산된 제1 암호화 행렬을 이용하여 암호화하여 상기 에지 서버 j에 전달하고, 상기 uCDN의 콘트롤 센터는 상기 제2 행 벡터를 콘텐츠 서비스 사업자의 개수의 크기를 갖는 벡터로 연산된 제2 암호화 행렬을 이용하여 암호화하여 상기 에지 서버 i에 전달하는 단계; 및

상기 에지 서버 j는 상기 제1 암호화 행렬의 역 행렬을 이용하여 상기 제1 행 벡터를 복호하고, 상기 에지 서버 i는 상기 제2 암호화 행렬의 역 행렬을 이용하여 상기 제2 행 벡터를 복호하는 단계를 더 포함하는 CDNi에서 CDN 사이에 암호화를 위한 키를 공유하는 방법.

발명의 설명

기 술 분 야

[0001] 이하 설명하는 기술은 CDNi에서 암호화를 위해 사용하는 키 공유 기법에 관한 것이다.

배 경 기 술

[0002] CDN(Content Delivery Network)은 사용자(end user)에게 콘텐츠를 효과적으로 전달하기 위해 사용된다. 콘텐츠 제공자는 CDN을 이용하여 사용자에게 콘텐츠를 제공한다. 복수의 CDN을 효과적으로 사용하기 위하여 CDNi(CDN Interconnection)가 제안되었다. CDNi는 복수의 독립적인 CDN을 일정한 인터페이스로 연결하고, 어떤 하나의 CDN이 다른 CDN을 대신하여 콘텐츠를 전달하는 네트워크이다. CDNi는 콘텐츠 서비스 제공자가 전세계상에서 사용자의 위치에 관계 없이 콘텐츠를 제공하는 서비스를 위한 것이다. 한편 CDNi가 취약할 수 있는 네트워크 공격(예컨대, DDoS 등)을 방어하기 위한 연구들도 진행되고 있다.

선행기술문헌

비특허문헌

[0003] (비특허문헌 0001) P. Giura, G. Reyes, "The security cost of content distribution network architectures," 35th IEEE Annual Computer Software and Applications Conference Workshops of IEEE Computer Society, pp. 128-135, 2011.

발명의 내용

해결하려는 과제

[0004] 이하 설명하는 기술은 SDN(Software Defined Network)와 ALTO(Application Layer Traffic Optimization) 서버를 사용하여 콘텐츠 요청을 라우팅하는 CDNi 네트워크를 제공하고자 한다. 이하 설명하는 기술은 ALTO 서버와 SDN에 기반하여 CDNi에서 대칭키를 생성하는 기법을 제공하고자 한다.

과제의 해결 수단

[0005] CDNi에서 CDN 사이에 암호화를 위한 키를 공유하는 방법은 CDNi를 구성하는 복수의 CDN에 각각 속한 에지 서버가 λ 크기의 열 벡터를 생성하는 단계, ALTO 서버가 상기 열 벡터 및 λ×λ 크기의 대칭 행렬의 집합 D'를 저장하는 단계, 상기 ALTO 서버는 uCDN의 에지 서버 i의 열 백터를 이용하여 블룸 기법에서 사용하는 제1 행 벡터

r_j를 생성하고, dCDN의 에지 서버 j에 대한 열 벡터를 이용하여 블롬 기법에서 사용하는 제2 행 벡터 r_i를 생성하는 단계, 상기 ALTO 서버는 상기 행 벡터 r_j를 상기 에지 서버 i에 전달하고, 상기 행 벡터 r_i를 상기 에지 서버 j에 전달하는 단계 및 상기 에지 서버 i는 자신이 생성한 열 백터와 상기 제1 행 벡터를 곱하여 제1 키를 생성하고, 상기 에지 서버 j는 자신이 생성한 열 벡터와 상기 제2 행 벡터를 곱하여 제2 키를 생성하는 단계를 포함한다.

발명의 효과

[0006] 이하 설명하는 기술은 ALTO 서버와 SDN을 기반으로 대칭키를 생성하여 CDNi의 보안성을 높인다.

도면의 간단한 설명

[0007] 도 1은 블롬 기법으로 한 쌍의 공유키를 생성하는 과정에 대한 예이다.

도 2는 CDNi 구조를 도시한 예이다.

도 3은 uCDN의 에지 서버와 dCDN의 에지 서버 사이의 대칭키 생성 및 분배 과정에 대한 절차 흐름도의 예이다.

발명을 실시하기 위한 구체적인 내용

[0008] 이하 설명하는 기술은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세하게 설명하고자 한다. 그러나, 이는 이하 설명하는 기술을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 이하 설명하는 기술의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0009] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 해당 구성요소들은 상기 용어들에 의해 한정되지는 않으며, 단지 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 이하 설명하는 기술의 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.

[0010] 본 명세서에서 사용되는 용어에서 단수의 표현은 문맥상 명백하게 다르게 해석되지 않는 한 복수의 표현을 포함하는 것으로 이해되어야 하고, "포함한다" 등의 용어는 설시된 특징, 개수, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 의미하는 것이지, 하나 또는 그 이상의 다른 특징들이나 개수, 단계 동작 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 배제하지 않는 것으로 이해되어야 한다.

[0011] 도면에 대한 상세한 설명을 하기에 앞서, 본 명세서에서의 구성부들에 대한 구분은 각 구성부가 담당하는 주기능 별로 구분한 것에 불과함을 명확히 하고자 한다. 즉, 이하에서 설명할 2개 이상의 구성부가 하나의 구성부로 합쳐지거나 또는 하나의 구성부가 보다 세분화된 기능별로 2개 이상으로 분화되어 구비될 수도 있다. 그리고 이하에서 설명할 구성부 각각은 자신이 담당하는 주기능 이외에도 다른 구성부가 담당하는 기능 중 일부 또는 전부의 기능을 추가적으로 수행할 수도 있으며, 구성부 각각이 담당하는 주기능 중 일부 기능이 다른 구성부에 의해 전담되어 수행될 수도 있음은 물론이다.

[0012] 또, 방법 또는 동작 방법을 수행함에 있어서, 상기 방법을 이루는 각 과정들은 문맥상 명백하게 특정 순서를 기재하지 않은 이상 명기된 순서와 다르게 일어날 수 있다. 즉, 각 과정들은 명기된 순서와 동일하게 일어날 수도 있고 실질적으로 동시에 수행될 수도 있으며 반대의 순서대로 수행될 수도 있다.

[0014] 이하 설명하는 기술은 CDNi 외에도 다양한 네트워크에서 대칭키 생성에 사용될 수 있다. 다만 설명의 편의를 위해 CDNi를 예로 설명하고자 한다. 이하 설명하는 기술은 CDNi에서 대칭키를 생성하는 기법이다. 이하 설명하는 기술은 SDN 및 ALTO 서버를 이용하여 효과적인 대칭키를 생성하는 기법이다. 또한 이하 설명하는 기술은 CDNi에서 대칭키를 사용하여 정보를 안전하게 전송하는 기법이다.

[0016] 이하 설명하는 대칭키 생성 기법은 기본적으로 블롬(Blom) 알고리즘에 기반한다. 따라서 먼저 블롬 기법에 대해 간략하게 설명한다. 블롬 기법은 네트워크에 위치하는 한 쌍의 노드가 사용할 수 있는 대칭키(symmetric secret

key)를 생성하고 분배하는 기법이다. 블롬 기법은 최대 λ개의 노드까지 대칭키를 생성할 수 있다. 이하 설명의 편의를 위해 대칭키를 생성하는 장치는 컴퓨팅 장치라고 명명한다.

[0017] 도 1은 블롬 기법으로 한 쌍의 공유키를 생성하는 과정에 대한 예이다. 블롬 기법은 유한한 필드인 GF(q) 상에 (λ+1)×N 크기의 행렬(matrix) G가 있다고 가정한다. N의 네트워크의 크기이고, GF(q)는 키의 크기(길이)에 충분한 소수이다. 컴퓨팅 장치는 GF(q) 상에 (λ+1)×(λ+1) 크기의 임의의 대칭 행렬 D를 생성하고, N×(λ+1) 크기의 행렬 $A = (D \cdot G)^T$를 연산한다. 여기서 T는 전치 연산을 의미한다. 즉 $(D \cdot G)^T$는 (D•G)의 전치 행렬이다. D는 보안이 유지되어야 한다. $(D \cdot G)^T$의 하나의 행은 각 사용자에게 공개(전달)된다. 여기서 사용자는 네트워크 장치를 사용하여 정보를 전달하는 주체를 의미한다. 이하 사용자는 동시에 해당 사용자가 사용하는 네트워크 장치와 동일한 의미이기도 한다. 예컨대, 사용자는 PC, 스마트폰 등과 같은 장치를 의미할 수 있다.

[0018] $D = D^T$이기 때문에 키 행렬(key matrix) $K = A \cdot G$는 아래의 수학식 1과 같이 연산될 수 있다.

수학식 1

[0020]
$$\boldsymbol{K} = A \cdot G = (D \cdot G)^T \cdot G = G^T \cdot D^T \cdot G = G^T \cdot D \cdot G$$
$$= G^T \cdot A^T = (A \cdot G)^T = \boldsymbol{K^T}$$

[0022] 수학식 1은 $K = A \cdot G$가 또한 대칭 행렬이라는 의미이다. 다른 말로 하면 $K_{ij} = K_{ji}$이다. K_{ij}는 K 행렬에서 i번째 행과 j번째 열을 의미한다. 따라서 K_{ij}와 K_{ji}는 사용자 i와 사용자 j 사이에 한 쌍의 공유키로 사용될 수 있다. 최종적으로 컴퓨팅 장치는 행렬 A의 k번째 행과 k번째 열 및 행렬 G의 k번째 행과 k번째 열을 각각 사용자 k(k = 1,...,N)에게 전달한다.

[0024] 이하 CDNi에서 보안성을 담보하기 위해 블롬 기법에 기반한 대칭키 생성 및 분배 기법을 설명한다. 또한 대칭키 생성에 보다 적합한 새로운 CDNi 구조에 대해서도 설명한다. 먼저 CDNi의 구조에 대하 설명한다.

[0026] **구조**

[0027] CDNi가 CDN와 다른 부분 중 하나는 업스트림 CDN(이하 uCDN)과 다운스트림 CDN(이하 dCDN) 사이의 요청 라우팅(request routing) 경로이다. 한편 SDN은 네트워크 서비스 제공자를 위한 프로그래밍 가능한 제어 플레인을 제공한다는 측면에서 새로운 네트워크 구조로 주목받고 있다. SDN은 기본적으로 애플리케이션 플레인(application plane), 제어 플레인(control plane) 및 데이터 플레인(data plane)을 갖는다. SDN의 구조 및 동작에 대한 자세한 설명은 생략한다. SDN은 CDNi를 위한 요청 라우팅(request routing) 결정하고 제어하기 위한 기법이 될 수 있다.

[0028] 도 2는 CDNi 구조(100)를 도시한 예이다. 도 2를 살펴보면, CDNi에는 서로 다른 네트워크 서비스 사업자(NSP)가 관리하는 서로 다른 CDN이 존재한다. 서로 다른 CDN은 일반적으로 서로 통신이 가능하다. CDN은 uCDN과 dCDN으로 분류할 수 있다. 사용자가 콘텐츠를 요청하면 해당 요청은 콘텐츠를 저장하고 있는 CDN으로 전달(redirection)된다. uCDN은 사용자 요청을 콘텐츠를 저장하고 있는 다른 CDN으로 전달하는 CDN이다. dCDN은 다른 CDN에 의하여 콘텐츠 요청을 전달받은 CDN이다. 도 2에서는 하나의 uCDN(140)과 두 개의 dCDN(120 및 130)을 도시하였다.

[0029] 하나 이상의 CDN이 동일한 콘텐츠를 저장(caching)할 수 있다. 따라서 CDNi에서는 어떤 CDN을 dCDN으로 결정할지가 중요하다. CDNi는 dCDN을 결정하는 과정(즉 콘텐츠를 제공할 라우팅을 결정하는 과정)을 ALTO 서버(110)와 함께 SDN을 사용하여 수행할 수 있다.

[0030] CDNi는 ALTO 서버(110) 및 복수의 CDN 노드(120, 130, 140)를 구비한다. 도 2에서는 CDN(120)의 콘트롤 센터(121), CDN(130)의 콘트롤 센터(131) 및 CDN(140)의 콘트롤 센터(141)를 도시하였다. 한편 각 CDN은 에지 서버를 갖는다. 도 2는 CDN(120)에 3개의 에지 서버(125)를 도시하였고, CDN(130)에 3개의 에지 서버(135)를 도시하였고, CDN(140)에 3개의 에지 서버(145)를 도시하였다. 각 CDN 노드는 콘텐츠를 저장하는 서버(에지 서버) 및 콘텐츠 전달 경로를 구성하는 스위치, 라우터를 포함할 수 있다.

[0031] CDN 노드는 CDNi 콘트롤러, ALTO 클라이언트 및 SDN 콘트롤러를 구비한다. 각 CDN 노드의 콘트롤러 센터(121, 131, 141)가 CDNi 콘트롤러, ALTO 클라이언트 및 SDN 콘트롤러를 포함한다. 도 2에서는 콘트롤러 센터(131)에 대해 대표적으로 CDNi 콘트롤러, ALTO 클라이언트 및 SDN 콘트롤러를 도시하였다.

[0033] CDNi 콘트롤러는 사용자의 콘텐츠 요청을 해당 CDN에 속한 가장 적절한 에지 서버로 전달(redirection)한다. 이 과정에서 CDNi 콘트롤러는 ALTO 클라이언트와 SDN 콘트롤러와 협력한다. CDNi 콘트롤러는 다른 CDNi 콘트롤러와 통신을 할 수 있다. CDNi 콘트롤러는 다른 CDNi 콘트롤러로부터 요청된 콘텐츠를 저장하고 있는 CDN에 대한 정보를 수신할 수 있다.

[0034] ALTO 서버(110)는 기본적으로 네트워크 정보를 ALTO 클라이언트에 제공한다. ALTO 클라이언트는 ALTO 서버(110)와 정보를 주고 받는 객체이다. ALTO 서버(110)는 네트워크의 구성, 네트워크의 위치, 네트워크의 경로 등과 같은 정보를 제공한다. ALTO 서버는 네트워크 맵(network map)과 비용 맵(cost map)을 보유한다. 네트워크 맵은 모든 CDN에 대한 네트워크 토폴로지에 대한 정보를 포함하고, 비용 맵은 경로를 구성하는 각 링크에 대한 거리 비용에 대한 정보를 포함한다. ALTO 클라이언트는 ALTO 서버(110)가 관리하는 맵을 이용하여 네트워크 정보를 제공 받는다.

[0035] ALTO 클라이언트는 사용자가 요청한 콘텐츠 요청을 ALTO 서버(110)에 전달할 수 있다. ALTO 서버(110)는 콘텐츠 요청을 기준으로 네트워크 토폴로지 및 비용을 고려하여 가장 적절한 라우팅 경로를 결정할 수 있다. ALTO 클라이언트는 전달한 요청에 대한 응답으로 콘텐츠 요청에 대해 가장 적절한 dCDN에 대한 정보(메타 데이터)를 수신할 수 있다. ALTO 클라이언트가 수신한 dCDN에 대한 메타 데이터는 CDNi 콘트롤러 및 SDN 콘트롤러에 전달된다.

[0036] CDNi에서 정보 전달에 대한 보안을 위해 도 2와 같이 ALTO 서버(110)가 보안 맵(security map)을 추가로 저장하고 관리할 수 있다. 보안 맵은 CDNi의 구성 요소 사이의 대칭 키를 생성하기 위한 정보를 저장한다. 이에 대해서는 후술한다.

[0037] dCDN에 대한 메타 데이터를 수신하고, uCDN의 CDNi 콘트롤러 및 dCDN의 CDNi 콘트롤러는 각각 요청받은 콘텐츠를 전달하기 위한 가장 적절한 에지 서버를 게이트웨이로 선택할 수 있다. SDN 콘트롤러는 두 개의 게이트웨이 사이의 경로를 설정할 수 있다. 따라서 콘텐츠는 dCDN의 게이트웨이에서 uCDN의 게이트웨이로 전달되고, uCDNi의 콘트롤러가 선택한 가장 가까운 uCDN의 에지 서버에 저장된다. 이후 사용자는 해당 uCDN의 에지 서버로부터 요청한 콘텐츠를 제공받게 된다. 이 과정에서 SDN 콘트롤러가 네트워크 공격으로부터 보호되어야 한다. 새로운 CDNi 구조는 SND 콘트롤러에 추가적인 페이로드(payload)를 사용할 수 있다.

[0039] **키 생성 및 분배 과정**

[0040] 전술한 콘텐츠 전달 과정을 정리하면 다음과 같다. 사용자가 특정 콘텐츠를 요청하면, CDN(uCDN)이 먼저 해당 요청을 수신하고 자신이 요청받은 콘텐츠를 보유하고 있지 않으면 다른 CDN(dCDN)으로 해당 요청을 전달한다. 그리고 uCDN은 가장 적절한 dCDN으로부터 콘텐츠를 수신하여 uCDN의 에지 서버(사용자에게 가장 가까운)에 저장한다. 최종적으로 사용자는 uCDN의 에지 서버로부터 콘텐츠를 제공받는다.

[0041] 상기 콘텐츠 전달 과정에서 콘텐츠는 서로 다른 CDNi의 구성 요소 사이에서 안전하게 전달되어야 한다. 도 2에서 해당 경로를 각 CDN 사이의 굵은 화살표로 도시하였다. 따라서 CDNi는 콘텐츠 암호화, 인증 등을 위해 키(key)를 사용해야 한다. CDNi의 특성상 현재 설정된 경로(예컨대, CDN 사이의 경로, 콘텐츠가 전달되는 경로 등)는 고정적이지 않다. 즉 통신 경로(link) 및 피어(peer)는 수시로 변경될 있다. 예컨대, CDNi 콘트롤 센터가 사용자를 위한 다른 에지 서버를 선택할 수도 있고, 트래픽을 고려하여 다른 uCDN을 선택할 수도 있기 때문이다. 즉, 이와 같이 정보가 전달되는 경로가 동적으로 변경되는 상황에 대응하는 동적인 대칭키가 필요하다. 대칭키는 dCDN으로부터 uCDN으로 콘텐츠를 전달(duplication)할 때 콘텐츠가 안전하게 전달되는 것을 보장할 수 있다.

[0043] 1) 대칭키 형성

[0044] 먼저 대칭키 형성에 이용하기 위한 기본 아이디어를 설명한다. 블롬 기법에 기반하여 다음과 같은 보조 정리를 도출할 수 있다.

[0045] 보조 정리(Lemma): D는 λ×λ 크기의 대칭 행렬이고, P는 임의의 λ×N 크기의 행렬이고, P^T는 P의 전치 행렬이다. D, P, P^T에 대해 $r(P^T)_i \cdot D \cdot c(P)_j = r(P^T)_j \cdot D \cdot c(P)_i$라는 관계를 갖는다. $r(P^T)_i$ 및 $r(P^T)_j$는 각각 행렬 P^T의 i번째 행 벡터이고, j번째 행 벡터이다. $c(P)_i$ 및 $c(P)_j$는 각각 행렁 P의 i번째 열 벡터이고, j번째 열 벡터이다. 이 보조 정리에 대한 증명은 다음과 같다.

[0046] 증명: P^T는 행렬 P의 전치 행렬이다. 따라서 $(c(P)_i)^T = r(P^T)_i$이고, $(r(P^T)_j)^T = c(P)_j$이다. D는 대칭 행렬이므로 $D = D^T$이다.

[0047]
$$
\begin{aligned}
r(P^T)_i \cdot D \cdot c(P)_j &= r(P^T)_i \cdot D \cdot c(P)_j \\
&= r(P^T)_i \cdot D^T \cdot r(P^T)_j{}^T \\
&= r(P^T)_i \cdot ((r(P^T)_j) \cdot D)^T \\
&= r(P^T)_i \cdot ((c(P)_j)^T \cdot D)^T \\
&= (c(P)_i)^T \cdot ((c(P)_j)^T \cdot D)^T \\
&= ((c(P)_j)^T \cdot D \cdot c(P)_i)^T \\
&= (r(P^T)_j \cdot D \cdot c(P)_i)^T
\end{aligned}
$$

[0048] 상기 수식에서 $r(P^T)_j$는 1×λ 행 벡터이고, D는 λ×λ행렬이고, $c(P)_i$는 λ×1 열 벡터이다. 따라서 $r(P^T)_j \cdot D \cdot c(P)_i$의 결과는 그 자신을 전치(transpose)한 값이고, $(r(P^T)_j \cdot D \cdot c(P)_i)^T = r(P^T)_j \cdot D \cdot c(P)_i$라는 관계를 갖는다. 결론적으로 아래의 수학식 2와 같이 정리될 수 있다.

수학식 2

[0050]
$$
r(P^T)_i \cdot D \cdot c(P)_j = r(P^T)_j \cdot D \cdot c(P)_i
$$

[0052] $K_{ij} = r(P^T)_i \cdot D \cdot c(P)_j$ 및 $K_{ji} = r(P^T)_j \cdot D \cdot c(P)_i$를 만들면, 결과는 $K_{ij} = K_{ji}$이다. 이를 통해 수학식 2와 같이 λ크기인 두 개의 열 벡터 및 λ×λ 크기의 대칭 행렬 D를 사용하여 한 쌍의 대칭키를 생성할 수 있다.

[0054] 2) 대칭키 분배

[0055] 상기 수학식 2를 사용하여 생성하는 대칭키를 전달하는 과정에 대해 설명한다.

[0056] 전술한 CDNi 구조와 관련하여 대칭키를 생성하데 사용하는 데이터를 마련하는 과정을 먼저 설명한다. CDN의 각 에지 서버는 λ크기인 임의의 열 벡터 $\bar{c}_i$를 생성한다. ALTO 서버는 다른 정보와 함께 에지 서버가 생성한 열 벡터에 대한 정보를 수집하여 전술한 보안 맵에 저장한다. 보안 맵은 열 벡터로 구성되는 벡터 풀(pool) P를 보유

하게 된다. 벡터 풀 P는 시간에 따라 새로운 열 벡터 요소로 업데이트 될 수 있다. 또한 보안 맵은 비밀 행렬 $D' = \{D_1, D_2, \ldots, D_m\}$ 및 H를 저장한다. D'는 전술한 대칭키 생성에 사용되는 대칭 행렬의 집합이다. H는 $k \times \lambda$ 크기의 행렬로서 각 행 벡터는 서로 다른 CDNi 콘트롤 센터에서 사용된다. k는 CDNi에 존재하는 CDN의 개수이다.

[0057] 새로운 CDNi 콘트롤 센터 x가 ALTO 서버에 등록되면, 새로운 행 벡터 $r(H)_x$가 행렬 H에 생성된다. ALTO 서버는 행 벡터 요소인 m으로 행 벡터 집합 r_{cdn_x}을 생성한다. r_{cdn_x}는 $\{r(H)_x \cdot D_1, \quad r(H)_x \cdot D_2, \quad \ldots, \quad r(H)_x \cdot D_m\}$ 와 같은 행 벡터 요소로 구성된다. ALTO 서버는 행 벡터 집합 r_{cdn_x}를 각 CDNi 콘트롤 센터 x로 전달한다. ALTO 서버는 다른 CDNi 콘트롤 센터에 대해서도 동일한 작업을 수행한다.

[0058] ALTO 서버와 CDNi에 존재하는 모든 에지 서버는 일 방향(irreversible) 함수 f()를 사전에 공유한다. ALTO 서버가 함수 f()를 각 에지 서버에 전달할 수 있다. 함수 f()는 아래의 수학식 3과 같이 열 벡터를 생성할 수 있다. 함수 f()는 에지 서버가 생성했던 열 벡터를 일정하게 가공(암호화)하는 함수에 해당한다.

수학식 3

[0060] $$c_i = f(ID, \bar{c}_i, TS)$$

[0061] 여기서 ID는 에지 서버의 식별자(번호)이다. $\bar{c}_i$는 에지 서버에서 생성되는 열 벡터이다. TS는 콘텐츠가 요청된 시점의 타임 스탬프(time stamp)이다.

[0063] uCDN의 에지 서버 i가 dCDN의 에지 서버 j로부터 콘텐츠를 수신하는 경우, 에지 서버 i 와 에지 서버 j사이에 한 쌍의 대칭키가 필요하다. 여기서 i및 j는 수학식 3에서의 ID에 해당한다. 이하 설명에서 에지 서버 i는 CDNi 콘트롤 센터 x가 관리하고, 에지 서버 j는 CDNi 콘트롤 센터 y가 관리하는 것으로 가정한다.

[0064] 도 3은 uCDN의 에지 서버와 dCDN의 에지 서버 사이의 대칭키 생성 및 분배 과정에 대한 절차 흐름도의 예이다. 도 3은 uCDN의 에지 서버 i와 dCDN의 에지 서버 j사이의 대칭키 생성 및 분배 과정에 해당한다. 이하 도 3을 기준으로 대칭키 생성 및 분배 과정에 대해 설명한다.

[0065] CDNi 콘트롤 센터 x는 dCDN으로부터 수신할 콘텐츠를 저장하기 위한 에지 서버 i를 선택한다(201). CDNi 콘트롤 센터 x는 자신의 ID와 TS를 ALTO 서버에 전달한다(202). ALTO 서버는 자신이 보유한 맵 정보를 이용하여 dCDN으로 CDNi 콘트롤 센터 y를 갖는 CDN을 선택한다(211). CDNi 콘트롤 센터 y는 콘텐츠를 uCDN에 전달한 에지 서버 j를 선택한다(221). 이제 에지 서버 i와 에지 서버 j 사이에 공유할 대칭키를 분배해야 할 것이다.

[0066] ALTO 서버는 아래의 과정을 통해 r_i' 및 r_j'를 생성한다(231).

[0067] ALTO 서버는 에지 서버 i가 생성한 열 벡터 $\bar{c}_i$ 및 에지 벡터 j가 생성한 열 벡터 $\bar{c}_j$를 보안 맵의 벡터 풀 P에서 찾는다. ALTO 서버는 상기 수학식 3을 적용하여 아래의 수학식 4와 같이 c_i 및 c_j를 연산한다.

수학식 4

[0069] $$c_i = f(ID_i, \bar{c}_i, TS)$$
$$c_j = f(ID_j, \bar{c}_j, TS)$$

[0071] 전술한 수학식 2에 따라 ALTO 서버는 아래의 수학식 5와 같이 에지 서버 j에 대한 행 벡터 r_i를 연산하고, 에지 서버 i에 대한 행 벡터 r_j를 각각 연산한다.

수학식 5

[0073]
$$r_i = (c_i)^T \cdot D$$
$$r_j = (c_j)^T \cdot D$$

[0075] ALTO 서버가 연산한 행 벡터 r_i 및 r_j는 수학식 1에서 설명한 블록 기법에서의 행렬 A의 행 벡터에 대응된다. 수학식 5에서 D는 ALTO 서버가 대칭 행렬의 집합 D'에서 선택한 어느 하나의 대칭 행렬이다.

[0076] ALTO 서버는 연산한 행 벡터 r_i를 CDNi 콘트롤 센터 y를 통해 에지 서버 j에 전달하고, 행 벡터 r_j 를 CDNi 콘트롤 센터 x를 통해 에지 서버 i에 전달한다. ALTO 서버는 행 벡터 r_i 및 r_j의 전송 전에 아래 수학식 6과 같이 가공(암호화)할 수 있다.

수학식 6

[0078]
$$r_i' = r_i + r(H)_y \cdot D_h$$
$$r_j' = r_j + r(H)_x \cdot D_k$$

[0080] ALTO 서버는 행 벡터 집합 r_{cdn_x}로부터 k번째 행 벡터 $r(H)_x \cdot D_k$를 선택하고, 행 벡터 집합 r_{cdn_y}로부터 h번째 행 벡터 $r(H)_y \cdot D_h$를 선택한다. 전술한 바와 같이 행 벡터 집합 r_{cdn_x}는 ALTO 서버가 CDNi 콘트롤 센터 x에 대해 생성했던 것이고, 행 벡터 집합 r_{cdn_y}는 ALTO 서버가 CDNi 콘트롤 센터 y에 대해 생성했던 것이다.

[0082] ALTO 서버는 r_i' 및 r_j'를 각각 CDNi 콘트롤 센터 y 및 CDNi 콘트롤 센터 x에 전달한다. 이때 ALTO 서버는 CDNi 콘트롤 센터 x에는 r_j 복호를 위한 k를 추가로 전달하고(232), DNi 콘트롤 센터 y에는 r_i복호를 위한 h를 추가로 전달한다(233).

[0083] CDNi 콘트롤 센터 y는 자신이 보유한(ALTO 서버가 사전에 송신했던) r_{cdn_y}로부터 h번째 행 벡터 $r(H)_y \cdot D_h$를 찾아 수신한 r_i'로부터 r_i를 추출한다(261). 또 CDNi 콘트롤 센터 x는 자신이 보유한 r_{cdn_x}로부터 k번째 행 벡터 $r(H)_x \cdot D_k$를 찾아 수신한 r_j'로부터 r_j를 추출한다(241).

[0084] 아래의 수학식 7과 같이 CDNi 콘트롤 센터 x는 r_j에 행렬 $O_{edge_server_i}$를 곱하고, 곱한 값 r_j''을 에지 서버 i에 전송한다(242). CDNi 콘트롤 센터 y는 r_i에 행렬 $O_{edge_server_j}$를 곱하고, 곱한 값 r_i''을 에지 서버 j에 전송한다(262).

수학식 7

[0086]
$$r_i'' = r_i \cdot O_{edge\_server\_j}$$
$$r_j'' = r_j \cdot O_{edge\_server\_i}$$

[0087] $O_{edge\_server\_i}$ 및 $O_{edge_server_j}$는 λ×λ 크기인 대각 행렬(diagonal matrix)이다. 대각 행렬은 대각선에 0이 아닌 요소가 존재한다. 아래 수학식 8과 같이 대각 행렬에서 0이 아닌 요소는 타임 스탬프(TS)와 각각 크기 β인 콘텐츠 저장 벡터 $V_{content\_stored\_i}$ 및 $V_{content_stored_j}$가 연산된 결과이다. β는 콘텐츠 서비스 사업자(CSP)의 숫자에 해당한다.

수학식 8

[0089]
$$O_{edge\_server\_i} = TS \lozenge V_{content\_stored\_i}$$

[0090] 수학식 8에서 ◊는 변환 연산자이다. 수학식 8에 의해 TS와 $V_{content_sotred_i}$는 0이 아닌 요소 λ개를 주 대각선에 갖는 λ×λ 크기의 대각 행렬을 생성한다. $V_{content_sotred_i}$의 요소 w는 해당 시점에서 에지 서버 i가 저장하고 있는 CSP w의 콘텐츠의 양에 해당한다. 에지 서버 i 및 CDNi 콘트롤 센터 x만 $V_{content_sotred_i}$를 보유하고 관리한다. 에지 서버 j 및 CDNi 콘트롤 센터 y는 $V_{content_sotred_j}$를 보유하고 관리한다.

[0091] 이후 아래 수학식 9와 같이 에지 서버 i는 CDNi 콘트롤 센터 x로부터 r_j''를 수신하고, 타임 스탬프(TS) 및 콘텐츠 저장 벡터 $V_{service_time_i}$로부터 역 행렬 $O_{edge_server_i}^{-1}$을 생성한다(251). 에지 서버 j는 CDNi 콘트롤 센터 y로부터 r_i''를 수신하고, 타임 스탬프(TS) 및 콘텐츠 저장 벡터 $V_{service_time_j}$로부터 역 행렬 $O_{edge_server_j}^{-1}$을 생성한다(271).

수학식 9

[0093]
$$r_i = r_i'' \cdot O_{edge\_server\_j}^{-1}$$
$$r_j = r_j'' \cdot O_{edge\_server\_i}^{-1}$$

[0095] 에지 서버 i 및 에지 서버 j는 각각 전술한 수학식 3을 이용하여 c_i 및 c_j를 연산할 수 있다. 전술한 보조 정리에 따라 대칭키는 아래의 수학식 10과 같이 생성될 수 있다.

수학식 10

[0097]
$$K_{ij} = r_i \cdot c_j = (c_i)^T \cdot D \cdot c_j$$
$$K_{ji} = r_j \cdot c_i = (c_j)^T \cdot D \cdot c_i$$

[0098] 보조 정리에 따라 $K_{ij} = K_{ji}$인 것을 알 수 있다. 결국 에지 서버 i 및 에지 서버 j는 한 쌍의 대칭키를 공유하게 된다(251 및 271).

[0100] 본 실시예 및 본 명세서에 첨부된 도면은 전술한 기술에 포함되는 기술적 사상의 일부를 명확하게 나타내고 있는 것에 불과하며, 전술한 기술의 명세서 및 도면에 포함된 기술적 사상의 범위 내에서 당업자가 용이하게 유추할 수 있는 변형 예와 구체적인 실시예는 모두 전술한 기술의 권리범위에 포함되는 것이 자명하다고 할 것이다.

부호의 설명

[0101] 100 : CDNi

110 : ALTO 서버

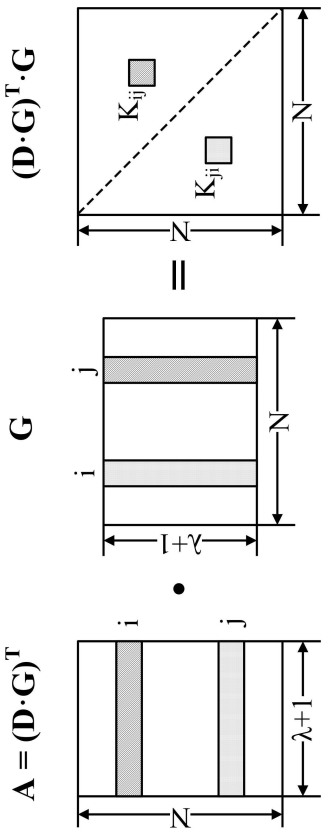
120, 130, 140 : CDN 노드

121, 131, 141 : CDN 콘트롤 센터

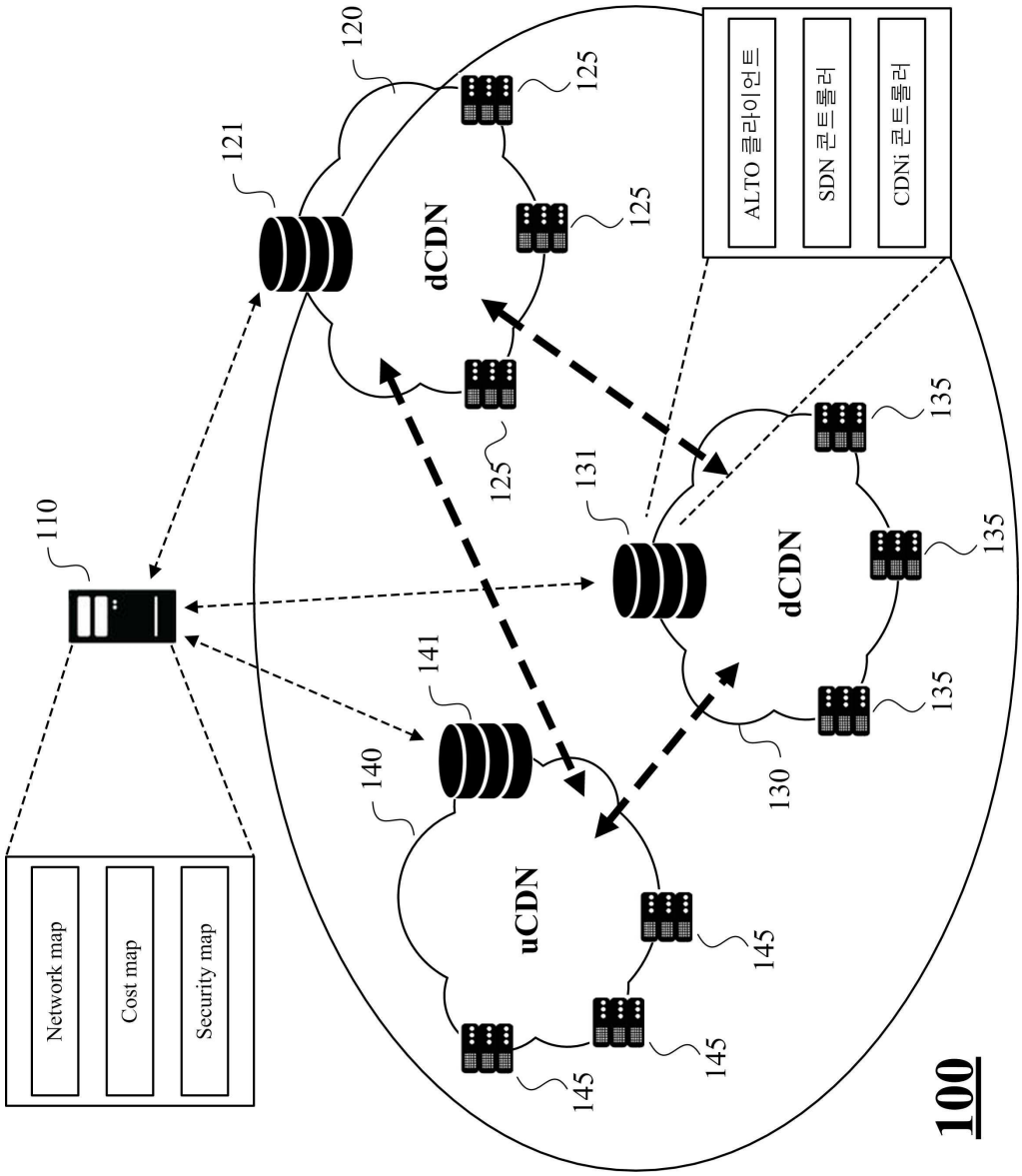
125, 135, 145 : 에지 서버

도면

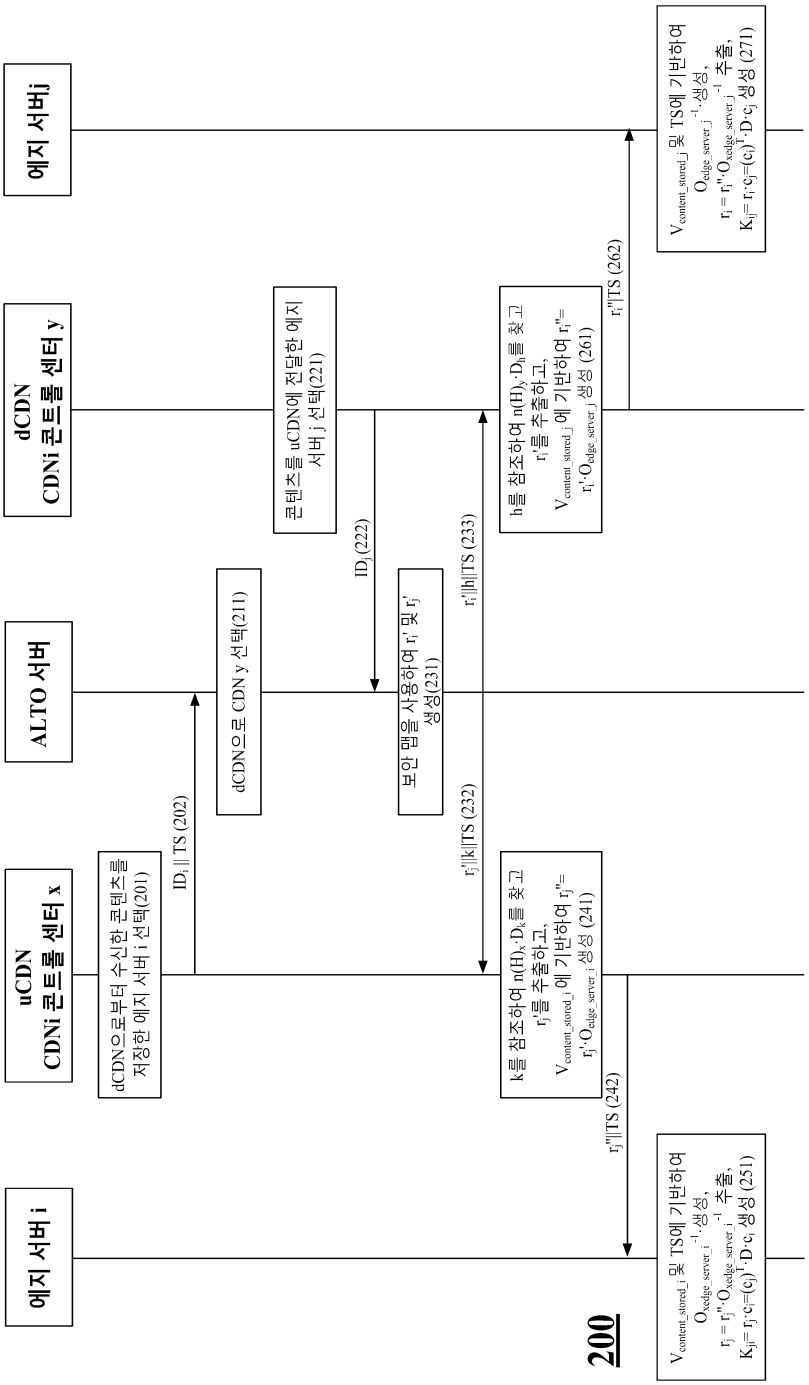
도면1



도면2


120
121
125
125
125
dCDN
ALTO 클라이언트
SDN 콘트롤러
CDNi 콘트롤러
110
131
135
135
135
dCDN
141
140
130
uCDN
145
145
145
Network map
Cost map
Security map
100

도면3


에지 서버 i
uCDN
CDNi 콘트롤 센터 x
ALTO 서버
dCDN
CDNi 콘트롤 센터 y
에지 서버j
dCDN으로부터 수신한 콘텐츠를 저장한 에지 서버 i 선택(201)
IDi || TS (202)
dCDN으로 CDN y 선택(211)
콘텐츠를 uCDN에 전달한 에지 서버 j 선택(221)
IDj (222)
보안 맵을 사용하여 ri' 및 rj' 생성(231)
ri'||h||TS (233)
rj'||k||TS (232)
k를 참조하여 n(H)x·Dk를 찾고 rj'를 추출하고, Vcontent_stored_i에 기반하여 rj"= rj'·Oedge_server_i 생성 (241)
h를 참조하여 n(H)y·Dh를 찾고 ri'를 추출하고, Vcontent_stored_j에 기반하여 ri"= ri'·Oedge_server_j 생성 (261)
ri"||TS (262)
rj"||TS (242)
Vcontent_stored_i 및 TS에 기반하여 Oxedge_server_i -1 생성, rj = rj"·Oxedge_server_i -1 추출, Kij= rj·cj=(cj)i·D·cj 생성 (251)
Vcontent_stored_j 및 TS에 기반하여 Oxedge_server_j -1 생성, ri = ri"·Oxedge_server_j -1 추출, Kij= ri·cj=(cj)i·D·cj 생성 (271)
200