



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년03월11일
(11) 등록번호 10-0888075
(24) 등록일자 2009년03월03일

(51) Int. Cl.

H04L 9/06 (2006.01) H04L 9/28 (2006.01)

(21) 출원번호 10-2008-0039171

(22) 출원일자 2008년04월28일

심사청구일자 2008년04월28일

(56) 선행기술조사문헌

KR1020050071625 A*

US20070028099 A1*

JP2008067102 A

WO2007044276 A2

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

인하대학교 산학협력단

인천 남구 용현동 253 인하대학교

(72) 발명자

권구인

경기도 부천시 소사구 범박동 현대홈타운 403동 703호

(74) 대리인

특허법인태동

전체 청구항 수 : 총 5 항

심사관 : 임대식

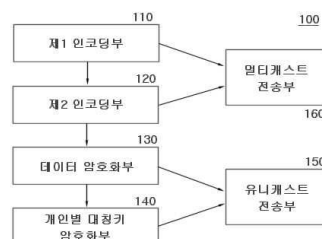
(54) 개인별 대칭키를 이용한 멀티캐스트를 위한 암호화 및복호화 시스템

(57) 요약

본 발명은 개인별 대칭키를 이용한 멀티캐스트를 위한 암호화 및 복호화 시스템으로서, 그 중 암호화 시스템은 (1) 전송하고자 하는 콘텐츠 데이터를 순방향 오류 수정(Forward Error Connection; FEC) 코드 방식으로 인코딩하는 제1 인코딩부; (2) 상기 제1 인코딩부에서 인코딩된 데이터 중 디코딩에 반드시 요구되는 데이터만을 FEC 방식으로 다시 한 번 인코딩하는 제2 인코딩부; (3) 상기 제2 인코딩부에서 인코딩된 데이터 중 디코딩에 반드시 요구되는 데이터만을 개인별 대칭키를 사용하여 암호화하는 데이터 암호화부; 및 (4) 상기 데이터 암호화부에서 사용된 상기 개인별 대칭키(Personal Symmetric Key)를 개인별 공개키를 사용하여 암호화하는 개인별 대칭키 암호화부를 포함하는 것을 그 구성상의 특징으로 한다. 또한, 복호화 시스템은 (1) 개인별 공개키로 암호화되어 수신된 개인별 대칭키를 개인키(Private Key)를 이용하여 복호화하는 개인별 대칭키 복호화부; (2) 상기 개인별 대칭키 복호화부에서 복호화된 개인별 대칭키를 이용하여 암호화되어 수신된 데이터를 복호화하는 데이터 복호화부; (3) 상기 데이터 복호화부에서 복호화된 데이터와 암호화되지 않은 채 수신된 데이터 중 일부 데이터를 함께 순방향 오류수정 코드(Forward Error Connection; FEC) 방식으로 디코딩하는 제1 디코딩부; 및 (4) 상기 제1 디코딩부에서 디코딩된 데이터와 암호화되지 않은 채 수신된 데이터 중 제1 디코딩부에서 디코딩되지 않은 나머지 데이터를 함께 FEC 방식으로 디코딩하는 제2 디코딩부를 포함하는 것을 그 구성상의 특징으로 한다.

본 발명에서 제안하고 있는 개인별 대칭키를 이용한 멀티캐스트를 위한 암호화 및 복호화 시스템에 따르면, 멀티캐스트 네트워크 환경에서 순방향 오류수정 코드(FEC) 방식을 이용하여 반복적으로 데이터를 인코딩한 후 인코딩된 데이터 중 디코딩에 반드시 필요한 데이터만을 개인별 대칭키를 이용하여 암호화함으로써, 암호화 비용을 최소화하면서 동시에 개인별 대칭키를 통해 각 개인들을 직접 관리할 수 있도록 하여 관리 비용을 최소화할 수 있다. 또한, 본 발명에서 제안하고 있는 개인별 대칭키를 이용한 멀티캐스트를 위한 암호화 및 복호화 시스템에 따르면, 암호화된 데이터와 암호화에 사용된 키를 직접 사용자에게 유니캐스트 방식으로 전송하기 때문에 사용자들을 직접 관리할 수 있으며, 나아가 개인별 키를 사용하여 미리 오프라인 방식으로 암호화를 실행할 수 있기 때문에, 서버에서 자원의 여유가 있는 경우 미리 암호화를 실행할 수 있다.

대 표 도 - 도1



특허청구의 범위

청구항 1

개인별 대칭키를 이용한 멀티캐스트용 암호화 시스템으로서,

- (1) 전송하고자 하는 콘텐츠 데이터를 순방향 오류 수정(Forward Error Connection; FEC) 코드 방식으로 인코딩하는 제1 인코딩부;
- (2) 상기 제1 인코딩부에서 인코딩된 데이터 중 디코딩에 반드시 요구되는 데이터만을 FEC 방식으로 다시 한 번 인코딩하는 제2 인코딩부;
- (3) 상기 제2 인코딩부에서 인코딩된 데이터 중 디코딩에 반드시 요구되는 데이터만을 개인별 대칭키를 사용하여 암호화하는 데이터 암호화부; 및
- (4) 상기 데이터 암호화부에서 사용된 상기 개인별 대칭키를 개인별 공개키를 사용하여 암호화하는 개인별 대칭키 암호화부;
- (5) 상기 데이터 암호화부에서 암호화된 데이터 및 상기 개인별 대칭키 암호화부에서 암호화된 개인별 대칭키를 유니캐스트(unicast) 방식으로 전송하는 유니캐스트 전송부; 및
- (6) 상기 제1 인코딩부에서 인코딩된 데이터 중 디코딩에 요구되는 데이터를 제외한 나머지 데이터 및 상기 제2 인코딩부에서 인코딩된 데이터 중 디코딩에 반드시 요구되는 데이터를 제외한 나머지 데이터를 함께 멀티캐스트(multicast) 방식으로 전송하는 멀티캐스트 전송부를 포함하는 것을 특징으로 하는 멀티캐스트용 암호화 시스템.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 제1 인코딩부에서 인코딩된 데이터 중 디코딩에 요구되는 데이터는 전체 데이터의 4%이고, 상기 제2 인코딩부에서 인코딩된 인코딩 데이터 중 디코딩에 요구되는 데이터는 0.16%인 것을 특징으로 하는 멀티캐스트용 암호화 시스템.

청구항 4

제1항에 있어서,

오프라인(offline) 방식으로 개인별 암호화를 미리 수행할 수 있는 것을 특징으로 하는 멀티캐스트용 암호화 시스템.

청구항 5

개인별 대칭키를 이용한 멀티캐스트용 복호화 시스템으로서,

- (1) 개인별 공개키로 암호화되어 유니캐스트(unicast)방식으로 전송된 개인별 대칭키를 수신하고, 상기 수신된 개인별 대칭키를 개인키를 이용하여 복호화하는 개인별 대칭키 복호화부;
- (2) 상기 개인별 대칭키를 이용하여 암호화되어 유니캐스트 방식으로 전송된 데이터를 수신하고, 상기 개인별 대칭키 복호화부에서 복호화된 개인별 대칭키를 이용하여 상기 수신된 데이터를 복호화하는 데이터 복호화부;
- (3) 암호화되지 않은 채 멀티캐스트(multicast) 방식으로 전송된 데이터 중 일부 데이터를 수신하고, 상기 수신된 일부 데이터와 상기 데이터 복호화부에서 복호화된 데이터를 함께 순방향 오류수정 코드(Forward Error Connection; FEC) 방식으로 디코딩하는 제1 디코딩부; 및
- (4) 상기 암호화되지 않은 채 멀티캐스트 방식으로 전송되는 데이터 중 상기 일부 데이터를 제외한 나머지 데이터를 수신하고, 상기 수신된 나머지 데이터와 상기 제1 디코딩부에서 디코딩된 데이터를 함께 FEC 방식으로 디

코딩하는 제2 디코딩부;

를 포함하는 멀티캐스트용 복호화 시스템.

청구항 6

삭제

청구항 7

제5항에 있어서,

암호화되어 수신된 상기 데이터는 전체 데이터의 0.16%이고, 암호화되지 않은 채 수신된 데이터 중 상기 제1 디코딩부에서 디코딩되는 상기 일부 데이터는 전체 데이터의 3.84%인 것을 특징으로 하는 멀티캐스트용 복호화 시스템.

명세서

발명의 상세한 설명

기술 분야

- <1> 본 발명은 개인별 대칭키를 이용한 멀티캐스트를 위한 암호화 및 복호화 시스템으로서, 보다 구체적으로는 멀티캐스트 네트워크 환경에서 순방향 오류수정 코드(FEC) 방식을 이용하여 반복적으로 데이터를 인코딩한 후 인코딩된 데이터 중 디코딩에 반드시 필요한 데이터만을 개인별 대칭키(Personal Symmetric Key)를 이용하여 암호화함으로써, 암호화 비용을 최소화하면서 동시에 개인별 대칭키를 통해 각 개인들을 직접 관리할 수 있도록 하여 관리 비용을 최소화하는 멀티캐스트를 위한 암호화 및 복호화 시스템에 관한 것이다.

배경 기술

- <2> 네트워크에서의 브로드캐스트 방식은 유니캐스트 방식에서부터 멀티캐스트 방식으로 연구가 진행되어 왔다. 멀티캐스트 방식에서는, 많은 수의 사용자가 동시에 같은 내용의 콘텐츠(contents)를 원할 경우, 서버가 1개의 콘텐츠만을 전송하고, 네트워크 라우터에서 필요에 따라 복사를 하여 전송을 함으로써, 많은 사용자들이 동시에 같은 데이터를 전송받게 된다. 멀티캐스트 방식에서 데이터 전송의 보안을 위하여, 서버는 모든 사용자가 공유하는 키(그룹 키; group key)를 사용하여 데이터를 암호화하여 전송한다. 그룹 키 없이는 데이터의 복호화가 불가능하기 때문에 데이터의 전송 보안을 보장할 수 있다.
- <3> 암호화에 사용된 키를 안전하게 사용자에게 전달하기 위하여 공개키 암호화 방식이 사용된다. 사용자는 암호화하는 데 사용될 키를 서버 및 다른 사용자에게 공개하며, 서버는 이 키를 사용하여 암호화를 수행한다. 암호화된 데이터는 사용자만이 가지고 있는 개인키(Private Key)를 이용하여 복호화한다. 즉 암호화를 하는 키와 복호화를 하는 키가 서로 다른 비대칭 키를 가지는 암호화 기법이다. 위에서 설명된 멀티캐스트 그룹 키를 안전하게 사용자에게 전송하기 위하여, 서버는 각 사용자의 공개키(Public Key)를 이용하여 개인별로 그룹 키를 암호화한 후 유니캐스트로 사용자에게 개별 전송한다. 사용자는 암호화된 그룹 키를 전송받고, 사용자의 개인키(Private Key)를 사용하여 그룹 키를 복호화한다. 사용자는 복호화된 그룹 키를 이용하여 데이터를 복호화하여 사용한다. 만약 새로운 사용자가 가입을 하면, 기존의 데이터를 복호화하지 못하게 하기 위하여 새로운 그룹 키를 사용하여 암호화를 수행하며, 이 새로운 그룹 키는 기존의 사용자 및 새로운 가입자에게 전송된다. 만약 사용자가 그룹을 탈퇴하면, 탈퇴한 사용자는 앞으로 전송되는 데이터를 복호화하여서는 안 되므로, 사용자의 그룹 탈퇴 시 새로운 그룹 키를 이용하여 다시 암호화를 수행하여야 하며, 이 새로운 그룹 키를 그룹에 남아 있는 모든 사용자들에게 각 개인별로 유니캐스트 방식으로 전송한다. 이와 같이, 모든 그룹 멤버들이 하나의 그룹 키를 공유하는 방법을 전체 그룹 암호화(Whole Group Encryption) 방법이라고 하는데, 앞서 살펴본 바와 같이 새로운 사용자의 그룹 가입 및 기존 사용자의 그룹 탈퇴 시 항상 그룹 키를 갱신하여야 한다는 문제점이 있다. 또한 기존의 방식에서는 만약 서버가 암호화를 미리 수행하였다면(오프라인 암호), 이미 암호화된 데이터는 복호화 후 새로운 그룹 키를 사용하여 다시 암호화를 하여야 하므로, 사용자의 가입, 탈퇴에 따라 그룹 키를 갱신하는 기존의 방법에서는 오프라인으로 미리 암호화를 할 수 없다는 문제점도 있다.
- <4> 멀티캐스트 통신의 경우 동일한 데이터가 목적지 주소가 개인이 아닌 그룹 주소로 전송되므로 트래픽을 가로채기가 쉽기 때문에 유니캐스트 통신보다 보안의 위협에 매우 취약하다. 기본적인 키 관리 방법인 전체 그룹 암호화

호화(Whole Group Encryption) 방식에서는 하나의 그룹 키를 사용하므로 데이터 전송에 좋은 효율을 보이지만, 앞서 설명한 바와 같이, 새로운 멤버가 가입하거나 기존 멤버가 탈퇴하게 되면, 그때마다 서버는 새로운 키를 사용하여 암호를 다시 하여야 하며 또한 모든 그룹 멤버에게 새로운 그룹 키를 전송해야만 하는 문제점이 있다. 또한 종래의 기술들은 패킷의 암호화가 100%가 되어야하기 때문에, 즉 모든 데이터를 암호화하기 때문에 데이터의 크기가 증가할수록 암호화 비용이 급격하게 증가한다는 문제점이 있다. 전체 그룹 암호화에서는 모든 데이터가 멀티캐스트로 전송이 되기 때문에, 사용자는 그룹에 가입 후 서버의 관리가 아닌 라우터에 의하여 데이터를 전송받는다. 즉 서버는 전송하는 데이터가 네트워크의 어떠한 경로를 통하여 어느 사용자에게 전달이 되는지에 관하여 관리가 불가능하다. 따라서 서버는 각 사용자를 직접 관리하기 어려우며 특히 그룹 키의 분배 후에는 각 사용자를 직접 관리 할 수 있는 방법이 없다. 그 결과, 종래 기술을 이용하는 것만으로는, 서버가 사용자에게 요금을 부과하는 과금 서비스, 또는 서버가 사용자들을 직접 제어하여야 하는 서비스 등을 구현하기 어렵다는 문제점이 있다.

<5> 종래 기술의 멀티캐스트 방식에서는 모든 사용자들은 서버가 전송하는 데이터를 모두 같이 수신을 하였기에 그룹 키를 사용하여 암호화를 하였고, 개인별 키를 이용하여 암호화를 할 수 없었다. 즉 개인별로 암호화를 하였다면 멀티캐스트를 이용할 필요성이 없었기에 멀티캐스트에서는 개인별 키를 이용한 방식을 고려하지 않았었다.

<6> 한편, 순방향 오류 수정(Forward Error Correction; FEC) 코드 방식은, 멀티캐스트 기반 네트워크에서 데이터 전송 중 패킷의 손실 시 클라이언트(client) 측에서 손실된 패킷의 재전송 없이 복구할 수 있도록 하는 블록 인코딩 전송 방법이다. 다시 말해, 콘텐츠 서버(Content Server)가 인코딩된 패킷을 전송하면, 데이터를 수신한 클라이언트 측에서 패킷의 손실이 발생하더라도 다른 인코딩된 패킷을 추가적으로 수신하면 원상태의 파일을 복구할 수 있다. 이와 같은 이유로, FEC는 클라이언트가 패킷의 손실을 스스로 복구할 수 있는 순방향 오류 수정 방식이라고 한다. 이때 디코딩을 수행하기 위하여 반드시 필요한 패킷들이 전체 패킷의 약 4%를 차지하며, 이 패킷들을 암호화하여 네트워크의 전송 보안을 보장할 수 있다.

발명의 내용

해결 하고자하는 과제

<7> 본 발명은 기존에 제안된 시스템들의 상기와 같은 문제점들을 해결하기 위해 제안된 것으로서, 멀티캐스트 네트워크 환경에서 순방향 오류수정 코드(FEC) 방식을 이용하여 반복적으로 데이터를 인코딩한 후 인코딩된 데이터 중 디코딩에 반드시 필요한 데이터만을 개인별 대칭키를 이용하여 암호화함으로써, 암호화 비용을 최소화하면서 동시에 개인별 암호화를 통해 각 개인들을 직접 관리할 수 있도록 하여 관리 비용을 최소화하는 멀티캐스트를 위한 암호화 및 복호화 시스템을 제공하는 것을 그 목적으로 한다.

과제 해결수단

<8> 상기한 목적을 달성하기 위한 본 발명의 특징에 따른, 개인별 대칭키를 이용한 멀티캐스트를 위한 암호화 시스템은,

<9> (1) 전송하고자 하는 콘텐츠 데이터를 순방향 오류 수정(Forward Error Connection; FEC) 코드 방식으로 인코딩하는 제1 인코딩부;

<10> (2) 상기 제1 인코딩부에서 인코딩된 데이터 중 디코딩에 반드시 요구되는 데이터만을 FEC 방식으로 다시 한 번 인코딩하는 제2 인코딩부;

<11> (3) 상기 제2 인코딩부에서 인코딩된 데이터 중 디코딩에 반드시 요구되는 데이터만을 개인별 대칭키를 사용하여 암호화하는 데이터 암호화부; 및

<12> (4) 상기 데이터 암호화부에서 사용된 상기 개인별 대칭키를 개인별 공개키를 사용하여 암호화하는 개인별 대칭키 암호화부를 포함하는 것을 그 구성상의 특징으로 한다.

<13> 바람직하게는, (5) 상기 데이터 암호화부에서 암호화된 데이터 및 상기 개인별 대칭키 암호화부에서 암호화된 개인별 대칭키를 유니캐스트(unicast) 방식으로 전송하는 유니캐스트 전송부; 및 (6) 상기 제1 인코딩부에서 인코딩된 데이터 중 디코딩에 요구되는 데이터를 제외한 나머지 데이터 및 상기 제2 인코딩부에서 인코딩된 데이터 중 디코딩에 반드시 요구되는 데이터를 제외한 나머지 데이터를 함께 멀티캐스트(multicast) 방식으로 전송하는 멀티캐스트 전송부를 더 포함할 수 있다.

- <14> 바람직하게는, 상기 제1 인코딩부에서 인코딩된 데이터 중 디코딩에 요구되는 데이터는 전체 데이터의 4%이고, 상기 제2 인코딩부에서 인코딩된 인코딩 데이터 중 디코딩에 요구되는 데이터는 0.16%인 것을 특징으로 한다.
- <15> 바람직하게는, 오프라인(offline) 방식으로 개인별 암호화를 미리 수행할 수 있는 것을 특징으로 한다.
- <16> 상기한 목적을 달성하기 위한 본 발명의 또 다른 특징에 따른, 개인별 대칭키를 이용한 멀티캐스트를 위한 복호화 시스템은,
- <17> (1) 개인별 공개키로 암호화되어 수신된 개인별 대칭키를 개인키를 이용하여 복호화하는 개인별 대칭키 복호화부;
- <18> (2) 상기 개인별 대칭키 복호화부에서 복호화된 개인별 대칭키를 이용하여 암호화되어 수신된 데이터를 복호화하는 데이터 복호화부;
- <19> (3) 상기 데이터 복호화부에서 복호화된 데이터와 암호화되지 않은 채 수신된 데이터 중 일부 데이터를 함께 순방향 오류수정 코드(Forward Error Connection; FEC) 방식으로 디코딩하는 제1 디코딩부; 및
- <20> (4) 상기 제1 디코딩부에서 디코딩된 데이터와 암호화되지 않은 채 수신된 데이터 중 제1 디코딩부에서 디코딩되지 않은 나머지 데이터를 함께 FEC 방식으로 디코딩하는 제2 디코딩부를 포함하는 것을 그 구성상의 특징으로 한다.
- <21> 바람직하게는, 암호화되어 수신된 상기 개인별 대칭키 및 상기 데이터는 유니캐스트(unicast) 방식으로 전송되며, 암호화되지 않은 채 수신된 데이터는 멀티캐스트(multicast) 방식으로 전송되는 것을 특징으로 한다.
- <22> 바람직하게는, 암호화되어 수신된 상기 데이터는 전체 데이터의 0.16%이고, 암호화되지 않은 채 수신된 데이터 중 상기 제1 디코딩부에서 디코딩되는 상기 일부 데이터는 전체 데이터의 3.84%인 것을 특징으로 한다.

효 과

- <23> 본 발명에서 제안하고 있는 개인별 대칭키를 이용한 멀티캐스트를 위한 암호화 및 복호화 시스템에 따르면, 멀티캐스트 네트워크 환경에서 순방향 오류수정 코드(FEC) 방식을 이용하여 반복적으로 데이터를 인코딩한 후 인코딩된 데이터 중 디코딩에 반드시 필요한 데이터만을 개인별 대칭키를 이용하여 암호화함으로써, 암호화 비용을 최소화하면서 동시에 개인별 대칭키를 통해 각 개인들을 직접 관리할 수 있도록 하여 관리 비용을 최소화할 수 있다. 또한, 본 발명에서 제안하고 있는 개인별 대칭키를 이용한 멀티캐스트를 위한 암호화 및 복호화 시스템에 따르면, 암호화된 데이터와 암호화에 사용된 키를 직접 사용자에게 유니캐스트 방식으로 전송하기 때문에 사용자들을 직접 관리할 수 있으며, 나아가 개인별 키를 사용하여 미리 오프라인 방식으로 암호화를 실행할 수 있기 때문에, 서버에서 자원의 여유가 있는 경우 미리 암호화를 실행할 수 있다.

발명의 실시를 위한 구체적인 내용

- <24> 이하에서는 첨부된 도면들을 참조하여, 본 발명에 따른 실시예에 대하여 상세하게 설명하기로 한다.
- <25> 도 1은 본 발명의 일 실시예에 따른 개인별 대칭키를 이용한 멀티캐스트를 위한 암호화 시스템의 구성을 나타내는 도면이다. 도 1에 도시된 바와 같이, 본 발명의 일 실시예에 따른 개인별 대칭키를 이용한 멀티캐스트를 위한 암호화 시스템(100)은, 제1 인코딩부(110), 제2 인코딩부(120), 데이터 암호화부(130), 및 개인별 대칭키 암호화부(140)를 포함한다. 또한, 도 1에 도시된 바와 같이, 본 발명의 일 실시예에 따른 개인별 대칭키를 이용한 멀티캐스트를 위한 암호화 시스템(100)은, 유니캐스트 전송부(150) 및 멀티캐스트 전송부(160)를 더 포함할 수 있다.
- <26> 제1 인코딩부(110)는 전송하고자 하는 콘텐츠 데이터를 순방향 오류 수정(Forward Error Connection; FEC) 코드 방식으로 인코딩하는 역할을 하며, 제2 인코딩부(120)는 제1 인코딩부(110)에서 인코딩된 데이터 중 디코딩에 반드시 요구되는 데이터만을 FEC 방식으로 다시 한 번 인코딩하는 역할을 한다. 본 발명의 일 실시예에서는 FEC 방식 중 이미 그 유효성이 입증된 토네이도(Tornado) 코드를 이용하여 디코딩에 반드시 필요한 인코딩 데이터가 약 4%가 되도록 인코딩 데이터를 생성한다. 인코딩된 데이터 중 데이터 디코딩의 중요 부분이라고 할 수 있는 약 4%의 인코딩 데이터는 클라이언트 측면에서 데이터를 복구하는데 반드시 필요한 핵심이다. 따라서 본 발명의 일 실시예에서는 상기 4%의 인코딩 데이터를 다시 한 번 인코딩하게 된다. 그 결과, 제1 인코딩부(110)에서 인코딩된 데이터 중 디코딩에 요구되는 데이터는 전체 데이터의 4%인 데 반하여, 제2 인코딩부(120)에서 인코딩된 데이터 중 디코딩에 요구되는 데이터는 전체 데이터의 0.16%(4% x 4%)에 불과하게 된다.

- <27> 데이터 암호화부(130)는 제2 인코딩부(120)에서 인코딩된 데이터 중 디코딩에 반드시 요구되는 데이터만을 개인별 대칭키를 사용하여 암호화하는 역할을 하며, 개인별 대칭키 암호화부(140)는 데이터 암호화부(130)에서 사용된 개인별 대칭키를 개인별 공개키를 사용하여 암호화하는 역할을 한다. 데이터 암호화부(130)에서 암호화에 사용하는 키는 서버가 개인별로 임의로 선택한 대칭키이며, 이와 같이 암호화된 데이터와 개인별 대칭키는 사용자에게 직접 유니캐스트로 전송할 수 있다. 이때 서버는 사용자별로 다른 대칭키(개인별 대칭키)를 사용하여 암호화를 한다. 개인별 대칭키를 각각의 사용자에게 안전하게 전송하기 위하여 서버는 개인별 대칭키 암호화부(140)에서 사용자의 공개키를 이용하여 개인별 대칭키를 암호화하여 전송한다. 본 발명에서 제안하고 있는 개인별 대칭키를 이용한 암호화 시스템에서는, 오프라인(offline) 방식으로 개인별 암호화를 미리 수행할 수도 있다.
- <28> 유니캐스트 전송부(150)는 데이터 암호화부(130)에서 암호화된 데이터 및 개인별 대칭키 암호화부(140)에서 암호화된 개인별 대칭키를 유니캐스트(unicast) 방식으로 전송하는 역할을 하며, 멀티캐스트 전송부(160)는 제1 인코딩부(110)에서 인코딩된 데이터 중 디코딩에 요구되는 데이터를 제외한 나머지 데이터 및 제2 인코딩부(120)에서 인코딩된 데이터 중 디코딩에 반드시 요구되는 데이터를 제외한 나머지 데이터를 함께 멀티캐스트(multicast) 방식으로 전송하는 역할을 한다.
- <29> 도 1에서는 인코딩 단계를 두 번 거치고 있으나, 인코딩 단계의 횟수가 두 번으로 제한되는 것은 아니다. 즉, 제2 인코딩부 이후에, 이전 인코딩부에서 인코딩된 데이터 중 디코딩에 반드시 요구되는 데이터만을 FEC 방식으로 다시 한 번 인코딩하는 추가 인코딩부를 적어도 하나 이상 더 포함할 수 있다. 이와 같이 함으로써, 인코딩된 데이터 중 디코딩에 요구되는 데이터의 크기를 추가적으로 더 감소시킬 수 있다. 추가 인코딩부가 적용될 경우, 데이터 암호화부(130)는, 추가 인코딩부에서 인코딩된 데이터 중 디코딩에 반드시 요구되는 데이터만을 암호화하게 된다.
- <30> 도 2는 본 발명의 일 실시예에 따른 개인별 대칭키를 이용한 멀티캐스트를 위한 암호화 시스템을 실제 멀티캐스트 통신에 적용한 것을 나타내는 도면이다. 제2 인코딩 단계(인코더 b)를 거친 패킷 중에서 총 패킷의 약 0.16%(A-1 부분)만이 암호화되어 유니캐스트 방식으로 각 사용자에게 전송된다. 데이터 암호화에 사용된 키는 서버가 임의(random)로 선택한 대칭키(개인별 대칭키)이며, 이때 사용된 키는 사용자 1명에게만 전송이 된다. 즉 서버는 개인별로 서로 다른 대칭키를 사용하여 암호화를 수행한다. 따라서 서버는 사용자의 수와 같은 개수의 키를 생성하여 암호화하며, 사용자들은 각자 고유한 키를 전송받는다. 개인별 대칭키를 사용자에게 안전하게 전송하기 위하여, 개인별 대칭키를 사용자의 공개키를 이용하여 암호화한 후, 사용자에게 유니캐스트 방식으로 전송한다. 나머지 약 99.84%의 암호화되지 않은 데이터에 대한 인코딩 패킷은 멀티캐스트 방식으로 전송된다.
- <31> 도 3은 본 발명의 일 실시예에 따른 개인별 대칭키를 이용한 멀티캐스트를 위한 복호화 시스템의 구성을 나타내는 도면이다. 도 1에 도시된 바와 같이, 본 발명의 일 실시예에 따른 개인별 대칭키를 이용한 멀티캐스트를 위한 복호화 시스템(300)은, 개인별 대칭키 복호화부(310), 데이터 복호화부(320), 제1 디코딩부(330), 및 제2 디코딩부(340)를 포함한다.
- <32> 개인별 대칭키 복호화부(310)는 개인별 공개키로 암호화되어 수신된 개인별 대칭키를 개인키를 이용하여 복호화하는 역할을 하며, 데이터 복호화부(320)는 개인별 대칭키 복호화부(310)에서 복호화된 개인별 대칭키를 이용하여 암호화되어 수신된 데이터를 복호화하는 역할을 한다. 본 발명의 일 실시예에서는, 암호화되어 수신된 개인별 대칭키 및 암호화되어 수신된 데이터는 유니캐스트 방식으로 전송되며, 암호화되지 않은 채 수신된 데이터는 멀티캐스트 방식으로 전송된다.
- <33> 제1 디코딩부(330)는 데이터 복호화부(320)에서 복호화된 데이터와 암호화되지 않은 채 수신된 데이터 중 일부 데이터를 함께 순방향 오류수정 코드(Forward Error Connection; FEC) 방식으로 디코딩하는 역할을 하며, 제2 디코딩부(340)는 제1 디코딩부(330)에서 디코딩된 데이터와 암호화되지 않은 채 수신된 데이터 중 제1 디코딩부(330)에서 디코딩되지 않은 나머지 데이터를 함께 FEC 방식으로 디코딩하는 역할을 한다. 본 발명의 일 실시예에서는 FEC 방식 중 이미 그 유효성이 입증된 토네이도(Tornado) 코드를 이용한다. 그 결과, 암호화되어 수신된 데이터는 전체 데이터의 0.16%에 불과하며, 암호화되지 않은 채 수신된 데이터 중 제1 디코딩부(330)에서 디코딩되는 일부 데이터는 전체 데이터의 3.84%에 해당한다.
- <34> 도 3에서는 디코딩 단계를 두 번 거치고 있으나, 디코딩 단계의 횟수가 두 번으로 제한되는 것은 아니다. 즉, 추가 인코딩부에 의해 추가적으로 인코딩된 데이터를 수신하는 경우, 이에 대응하여 추가 디코딩부를 더 포함할

수 있다.

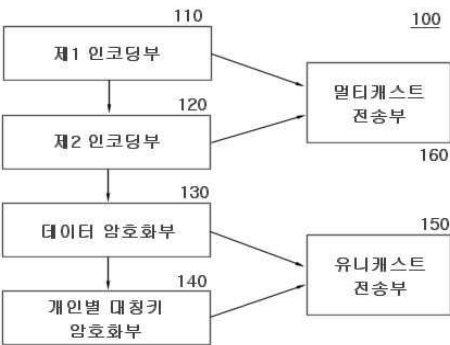
- <35> 도 4는 본 발명의 일 실시예에 따른 개인별 대칭키를 이용한 멀티캐스트를 위한 복호화 시스템을 실제 멀티캐스트 방송에 적용한 것을 나타내는 도면이다. 즉, 도 4에서는 클라이언트가 유니캐스트 방식으로 전송받은 약 0.16%의 암호화 데이터를 복호화한 후 디코딩하는 절차를 보여준다. 먼저, 사용자는 자신의 개인키를 이용하여 암호화된 개인별 대칭키를 복호화한다. 개인별 대칭키가 복호화되면, 사용자는 이를 이용하여 암호화된 데이터를 복호화한다. 이렇게 복호화된 데이터(A-1 부분)는 제1 디코딩부(디코더 b)에 필요한 데이터(A-2 부분)와 함께 디코딩되어 A 부분의 데이터를 생성한다. 생성된 A 부분의 데이터는 B 부분의 데이터와 함께 제2 디코딩부(디코더 a)에 의해 디코딩되어 최초의 콘텐츠를 복원하게 된다.
- <36> 이상 설명한 본 발명은 본 발명이 속한 기술분야에서 통상의 지식을 가진 자에 의하여 다양한 변형이나 응용이 가능하며, 본 발명에 따른 기술적 사상의 범위는 아래의 특허청구범위에 의하여 정해져야 할 것이다.

도면의 간단한 설명

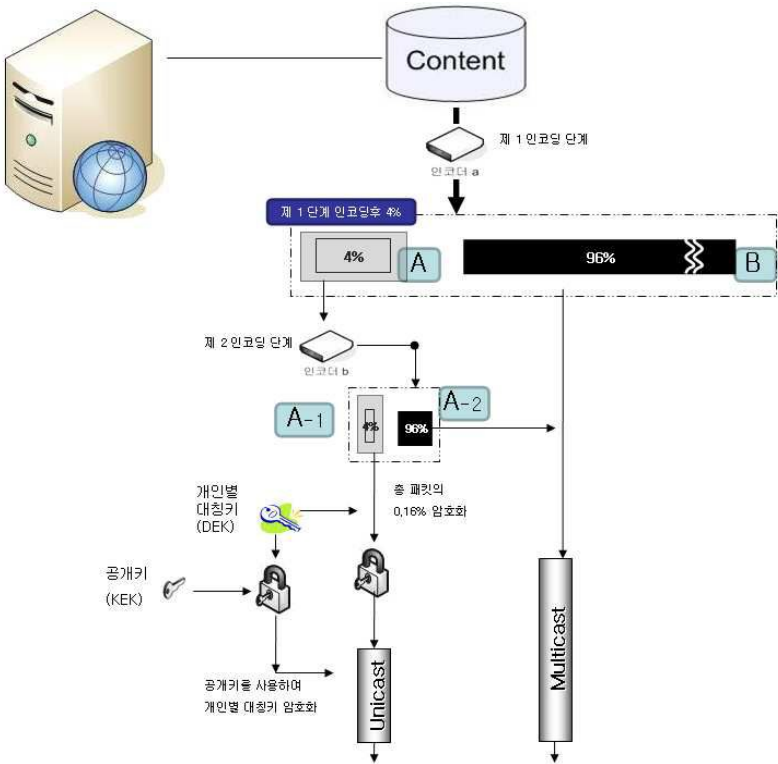
- <37> 도 1은 본 발명의 일 실시예에 따른 개인별 대칭키를 이용한 멀티캐스트를 위한 암호화 시스템의 구성을 나타내는 도면.
- <38> 도 2는 본 발명의 일 실시예에 따른 개인별 대칭키를 이용한 멀티캐스트를 위한 암호화 시스템을 실제 멀티캐스트 통신에 적용한 것을 나타내는 도면.
- <39> 도 3은 본 발명의 일 실시예에 따른 개인별 대칭키를 이용한 멀티캐스트를 위한 복호화 시스템의 구성을 나타내는 도면. 도 1에 도시된 바와 같이, 본 발명의 일 실시예에 따른 개인별 대칭키를 이용한 멀티캐스트를 위한 복호화 시스템(300)은, 개인별 대칭키 복호화부(310), 데이터 복호화부(320), 제1 디코딩부(330), 및 제2 디코딩부(340)를 포함한다.
- <40> 도 4는 본 발명의 일 실시예에 따른 개인별 대칭키를 이용한 멀티캐스트를 위한 복호화 시스템을 실제 멀티캐스트 방송에 적용한 것을 나타내는 도면.
- <41> <도면 중 주요 부분에 대한 부호의 설명>
- <42> 100: (본 발명의 일 실시예에 따른) 개인별 대칭키를 이용한 멀티캐스트를 위한 암호화 시스템
- <43> 110: 제1 인코딩부
- <44> 120: 제2 인코딩부
- <45> 130: 데이터 암호화부
- <46> 140: 개인별 대칭키 암호화부
- <47> 150: 유니캐스트 전송부
- <48> 160: 멀티캐스트 전송부
- <49> 300: (본 발명의 일 실시예에 따른) 개인별 대칭키를 이용한 멀티캐스트를 위한 복호화 시스템
- <50> 310: 개인별 대칭키 복호화부
- <51> 320: 데이터 복호화부
- <52> 330: 제1 디코딩부
- <53> 340: 제2 디코딩부

도면

도면1



도면2



도면3



도면4

