(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년02월20일
(11) 등록번호 10-1365603
(24) 등록일자 2014년02월14일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01) *H04L 9/28* (2006.01)
(21) 출원번호 10-2007-0031139
(22) 출원일자 2007년03월29일
심사청구일자 2012년03월29일
(65) 공개번호 10-2008-0050934
(43) 공개일자 2008년06월10일
(30) 우선권주장
60/872,506 2006년12월04일 미국(US)
(56) 선행기술조사문헌
KR1020060118247 A
US20060126848 A1
US20060041752 A1
US20040172550 A1

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
유용국
서울특별시 성동구 독서당로 272, 대우아파트 101동 1402호 (금호동4가)
야오준
경기도 수원시 영통구 덕영대로1555번길 20, 벽적골9단지아파트 943동 1405호 (영통동)
이충훈
서울특별시 관악구 남부순환로187길 19, 302호 (신림동)
(74) 대리인
리앤목특허법인

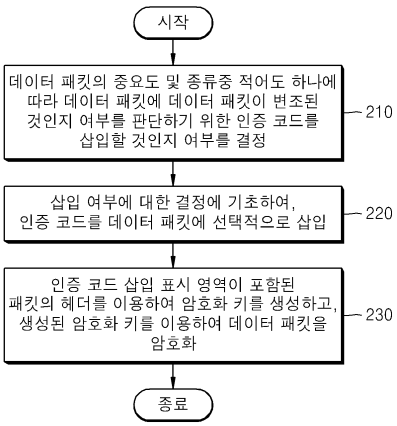
전체 청구항 수 : 총 33 항 심사관 : 이병수

(54) 발명의 명칭 **조건부 인증 코드 삽입 방법 및 그 장치, 인증을 통한조건부 데이터 사용 방법 및 그 장치**

(57) 요 약

본 발명은 조건부 인증 코드 삽입 방법에 관한 것으로, 데이터 패킷의 중요도 및 종류 중 적어도 하나에 따라 데이터 패킷에 데이터 패킷이 변조된 것인지 여부를 판단하기 위한 인증 코드를 삽입할 것인지 여부를 결정하고, 그 결정에 기초하여, 인증 코드를 데이터 패킷에 선택적으로 삽입함으로써, 데이터에 대한 효율적인 인증을 수행할 수 있다.

대 표 도 - 도2



특허청구의 범위

청구항 1

조건부 인증 코드 삽입 방법에 있어서,

데이터 패킷의 중요도 및 종류 중 적어도 하나에 따라 상기 데이터 패킷에 상기 데이터 패킷이 변조된 것인지 여부를 판단하기 위한 인증 코드를 삽입할 것인지 여부를 결정하는 단계; 및

상기 결정에 기초하여, 상기 인증 코드를 상기 데이터 패킷에 선택적으로 삽입하는 단계를 포함하는 것을 특징으로 하는 인증 코드 삽입 방법.

청구항 2

제1항에 있어서,

상기 결정하는 단계는

상기 데이터 패킷의 중요도 및 상기 데이터 패킷의 종류 중 적어도 하나에 따라 상기 패킷에 상기 인증 코드를 삽입할 것인지 여부에 대한 정보 또는 삽입 여부에 대한 판단 기준을 저장하고 있는 데이터베이스에 기초하여 상기 삽입 여부를 결정하는 것을 특징으로 하는 인증 코드 삽입 방법.

청구항 3

제1항에 있어서,

상기 데이터 패킷은 상기 패킷의 헤더가 상기 데이터 패킷이 상기 인증 코드가 삽입된 패킷인지를 표시하는 인증 코드 삽입 표시 영역을 포함하는 것을 특징으로 하는 인증 코드 삽입 방법.

청구항 4

제3항에 있어서,

상기 인증 코드 삽입 표시 영역이 포함된 상기 패킷의 헤더를 이용하여 암호화 키를 생성하고, 상기 생성된 암호화 키를 이용하여 상기 데이터 패킷을 암호화하는 단계를 더 포함하는 것을 특징으로 하는 인증 코드 삽입 방법.

청구항 5

제1항에 있어서,

상기 데이터 패킷이 인증 코드가 삽입된 패킷인지 여부에 따라 서로 다른 암호화 알고리즘을 이용하여 상기 데이터 패킷을 암호화하는 단계를 더 포함하는 것을 특징으로 하는 인증 코드 삽입 방법.

청구항 6

제1항에 있어서,

상기 결정하는 단계는

상기 데이터 패킷의 중요도가 높게 설정된 경우에는 상기 데이터 패킷에 상기 인증 코드를 삽입하고, 그 외의 경우에는 상기 데이터 패킷에 상기 인증 코드를 삽입하지 않도록 결정하는 것을 특징으로 하는 인증 코드 삽입 방법.

청구항 7

제1항에 있어서,

상기 결정하는 단계는

상기 데이터 패킷이 압축된 데이터인 경우에는 상기 인증 코드를 삽입하고, 상기 데이터 패킷이 비압축 데이터인 경우에는 상기 데이터 패킷에 상기 인증 코드를 삽입하지 않도록 결정하는 것을 특징으로 하는 인증

코드 삽입 방법.

청구항 8

제1항에 있어서,

상기 인증 코드는 비밀 키로 암호화된 CRC(cyclic redundancy checking)코드로 구성되는 것을 특징으로 하는 인증 코드 삽입 방법.

청구항 9

제1항에 있어서,

상기 인증 코드는 비밀 키드로 암호화된 HASH 또는 MAC 함수를 이용하여 생성된 인증 코드로 구성되는 것을 특징으로 하는 인증 코드 삽입 방법.

청구항 10

인증을 통한 조건부 데이터 사용 방법에 있어서,

데이터 패킷을 수신하고, 상기 수신된 데이터 패킷에 상기 데이터 패킷이 변조된 것인지 여부를 판단하기 위한 인증 코드가 삽입되었는지 여부를 판단하는 단계;

상기 데이터 패킷에 상기 인증 코드가 삽입되었다고 판단되는 경우에는 상기 인증을 수행하고, 상기 데이터 패킷에 상기 인증 코드가 삽입되지 않았다고 판단되는 경우에는 상기 인증을 수행하지 않는 단계; 및

상기 인증 수행 여부 및 상기 인증 수행 결과에 기초하여, 상기 데이터 패킷을 선택적으로 사용하는 단계를 포함하는 것을 특징으로 하는 데이터 사용 방법.

청구항 11

제10항에 있어서,

상기 판단하는 단계는

상기 데이터 패킷의 중요도 및 상기 데이터 패킷의 종류 중 적어도 하나에 따라 상기 패킷에 상기 인증 코드를 삽입할 것인지 여부에 대한 정보 또는 상기 삽입 여부에 대한 판단 기준을 저장하고 있는 데이터베이스에 기초하여 상기 삽입 여부를 판단하는 것을 특징으로 하는 데이터 사용 방법.

청구항 12

제10항에 있어서,

상기 판단하는 단계는

상기 데이터 패킷이 상기 인증 코드가 삽입된 패킷인지를 표시하는 상기 패킷의 헤더의 인증 코드 삽입 표시 영역에 기초하여 상기 삽입 여부를 판단하는 것을 특징으로 하는 데이터 사용 방법.

청구항 13

제10항에 있어서,

상기 판단하는 단계는

상기 데이터 패킷을 암호화한 알고리즘의 종류에 따라 상기 삽입 여부를 판단하는 것을 특징으로 하는 데이터 사용 방법.

청구항 14

제10항에 있어서,

상기 수신된 데이터 패킷에 에러가 있는 경우에는 상기 에러가 있는 데이터 패킷을 재수신하는 단계를 더 포함하는 것을 특징으로 하는 데이터 사용 방법.

청구항 15

제14항에 있어서,

상기 재수신하는 단계는

상기 데이터 패킷에 상기 인증 코드가 삽입되었는지 여부에 따라 상기 재수신 횟수를 달리하여 상기 데이터 패킷을 재수신하는 것을 특징으로 하는 데이터 사용 방법.

청구항 16

삭제

청구항 17

제10항에 있어서,

상기 데이터 패킷을 선택적으로 사용하는 단계는

상기 인증이 수행되지 않은 데이터 패킷 및 상기 인증 수행 결과 변조되지 않았다고 판단된 데이터 패킷은 사용하고, 그외의 데이터 패킷은 사용하지 않는 것을 특징으로 하는 데이터 사용 방법.

청구항 18

조건부 인증 코드 삽입 장치에 있어서,

데이터 패킷의 중요도 및 종류 중 적어도 하나에 따라 상기 데이터 패킷에 상기 데이터 패킷이 변조된 것인지 여부를 판단하기 위한 인증 코드를 삽입할 것인지 여부를 결정하는 인증 코드 삽입 결정부; 및

상기 결정에 기초하여, 상기 인증 코드를 상기 데이터 패킷에 선택적으로 삽입하는 인증 코드 삽입부를 포함하는 것을 특징으로 하는 인증 코드 삽입 장치.

청구항 19

제18항에 있어서,

상기 인증 코드 삽입 결정부는

상기 데이터 패킷의 중요도 및 상기 데이터 패킷의 종류 중 적어도 하나에 따라 상기 패킷에 상기 인증 코드를 삽입할 것인지 여부에 대한 정보 또는 상기 삽입 여부에 대한 판단 기준을 저장하고 있는 데이터베이스에 기초하여 상기 삽입 여부를 결정하는 것을 특징으로 하는 인증 코드 삽입 장치.

청구항 20

제18항에 있어서,

상기 데이터 패킷은 상기 패킷의 헤더가 상기 데이터 패킷이 상기 인증 코드가 삽입된 패킷인지를 표시하는 인증 코드 삽입 표시 영역을 포함하고, 상기 인증 코드 삽입부는 상기 인증 코드 삽입 표시 영역에 상기 패킷이 상기 인증 코드가 삽입된 패킷인지를 표시하는 것을 특징으로 하는 인증 코드 삽입 장치.

청구항 21

제20항에 있어서,

상기 인증 코드 삽입 표시 영역이 포함된 상기 패킷의 헤더를 이용하여 암호화 키를 생성하고, 상기 생성된 암호화 키를 이용하여 상기 데이터 패킷을 암호화하는 암호화부를 더 포함하는 것을 특징으로 하는 인증 코드 삽입 장치.

청구항 22

제21항에 있어서,

상기 암호화부는

상기 데이터 패킷이 인증 코드가 삽입된 패킷인지 여부에 따라 서로 다른 암호화 알고리즘을 이용하여 상기 데이터 패킷을 암호화하는 것을 특징으로 하는 인증 코드 삽입 장치.

청구항 23

제18항에 있어서,

상기 인증 코드 삽입 결정부는

상기 데이터 패킷의 중요도가 높게 설정된 경우에는 상기 데이터 패킷에 상기 인증 코드를 삽입하고, 그 외의 경우에는 상기 데이터 패킷에 상기 인증 코드를 삽입하지 않도록 결정하는 것을 특징으로 하는 인증 코드 삽입 장치.

청구항 24

제18항에 있어서,

상기 인증 코드 삽입 결정부는

상기 데이터 패킷이 압축된 데이터인 경우에는 상기 인증 코드를 삽입하고, 상기 데이터 패킷이 비압축 데이터인 경우에는 상기 데이터 패킷에 상기 인증 코드를 삽입하지 않도록 결정하는 것을 특징으로 하는 인증 코드 삽입 장치.

청구항 25

제18항에 있어서,

상기 인증 코드는 비밀 키로 암호화된 CRC(cyclic redundancy checking)코드로 구성되는 것을 특징으로 하는 인증 코드 삽입 장치.

청구항 26

제18항에 있어서,

상기 인증 코드는 비밀 키로 암호화된 HASH 또는 MAC 함수를 이용하여 생성된 인증 코드로 구성되는 것을 특징으로 하는 인증 코드 삽입 장치.

청구항 27

인증을 통한 조건부 데이터 사용 장치에 있어서,

데이터 패킷을 수신하는 수신부;

상기 수신된 데이터 패킷에 상기 데이터 패킷이 변조된 것인지 여부를 판단하기 위한 인증 코드가 삽입되었는지 여부를 판단하는 인증 코드 삽입 판단부;

상기 데이터 패킷에 상기 인증 코드가 삽입되었다고 판단되는 경우에는 상기 인증을 수행하고, 상기 데이터 패킷에 상기 인증 코드가 삽입되지 않았다고 판단되는 경우에는 상기 인증을 수행하지 않는 인증부; 및

상기 인증 수행 여부 및 상기 인증 수행 결과에 기초하여, 상기 데이터 패킷을 선택적으로 사용하는 데이터 사용부를 포함하는 것을 특징으로 하는 데이터 사용 장치.

청구항 28

제27항에 있어서,

상기 인증 코드 삽입 판단부는

상기 데이터 패킷의 중요도 및 상기 데이터 패킷의 종류 중 적어도 하나에 따라 상기 패킷에 상기 인증 코드를 삽입할 것인지 여부에 대한 정보 또는 상기 삽입 여부에 대한 판단 기준을 저장하고 있는 데이터베이스에 기초하여 상기 삽입 여부를 판단하는 것을 특징으로 하는 데이터 사용 장치.

청구항 29

제27항에 있어서,

상기 인증 코드 삽입 판단부는

상기 데이터 패킷이 상기 인증 코드가 삽입된 패킷인지를 표시하는 상기 패킷의 헤더의 인증 코드 삽입 표시 영역에 기초하여 상기 삽입 여부를 판단하는 것을 특징으로 하는 데이터 사용 장치.

청구항 30

제27항에 있어서,

상기 인증 코드 삽입 판단부는

상기 데이터 패킷을 암호화한 알고리즘의 종류에 따라 상기 삽입 여부를 판단하는 것을 특징으로 하는 데이터 사용 장치.

청구항 31

제27항에 있어서,

상기 수신된 데이터 패킷에 에러가 있는지를 검출하는 데이터 에러 검출부를 더 포함하고,

상기 수신부는 상기 수신된 데이터 패킷에 에러가 있는 경우에는 상기 에러가 있는 데이터 패킷을 재수신하는 것을 특징으로 하는 데이터 사용 장치.

청구항 32

제31항에 있어서,

상기 수신부는

상기 데이터 패킷에 인증 코드가 삽입되었는지 여부에 따라 재수신 횟수를 달리하여 상기 데이터 패킷을 재수신하는 것을 특징으로 하는 데이터 사용 장치.

청구항 33

삭제

청구항 34

제27항에 있어서,

상기 데이터 사용부는

상기 인증이 수행되지 않은 데이터 패킷 및 상기 인증 수행 결과 변조되지 않았다고 판단된 데이터 패킷은 사용하고, 그외의 데이터 패킷은 사용하지 않는 것을 특징으로 하는 데이터 사용 장치.

청구항 35

제1항 내지 제9항 및 제10항 내지 제17항 중 어느 한 항의 방법을 실행시키기 위한 프로그램이 기록된 컴퓨터로 읽을 수 있는 기록 매체.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0005] 본 발명은 조건부 인증 코드 삽입 방법 및 그 장치, 인증을 통한 조건부 데이터 사용 방법 및 그 장치에 관한 것이다.

[0006] 최근 수십 GHz대역을 이용하여 수 Gbps 전송율을 갖는 무선 송수신 시스템을 통해서 비압축 비디오/오디오 데이

터를 송수신하고자 하는 요구가 증가하고 있다. 이때, 컨텐츠를 보호하기 위하여 암호화가 필요한데 이와 같은 환경에서는 전송 속도가 빠르기 때문에 스트림 암호화 알고리즘이 블록암호화 알고리즘에 비해 유리하다.

[0007] 스트림(stream) 암호화 알고리즘은 임의의 난수 비트(bit) 열인 키 스트림(Key Stream)을 생성하여, 평문(plain text) 데이터에 비트 단위로 배타적 논리합 연산을 수행하는 방법으로 암호문을 생성한다.

[0008] 즉, 송신자가 평문 P와 키 스트림 K에 대하여 배타적 논리 합 연산(XOR: exclusive or)을 수행하여 암호문 C(=P XOR K)를 생성하여 보내면, 수신자는 암호문 C와 키 스트림 K에 대하여 배타적 논리 합 연산을 수행하여 평문 P(= C XOR K)를 도출한다.

[0009] 하지만, 이러한 방식 때문에 중간에서 공격자가 간단히 원래의 평문을 위조할 수 있다. 즉, 암호문 C = P XOR K를 중간에서 공격자가 간단히 P'을 XOR한다면 수신자는 C' = C XOR P'을 암호문으로 받게 되고 수학식 1에서와 같이 원래의 평문 P 대신 P XOR P'을 얻게 된다.

[0010] [수학식 1]

[0011] C' XOR K = C XOR P' XOR K = P XOR K XOR P' XOR K = P XOR P'

[0012] 따라서, 이러한 임의 변조를 막기 위하여, 데이터에 인증 값을 추가하여 보내주게 된다. 즉, 이 값의 확인을 통하여 중간에 데이터가 변조되지 않았음을 확인하게 되는 것이다. 이것을 위해서는 여러 가지 방법이 사용될 수 있는데 MAC(Message Authentication Code)과 같이 비밀키를 사용한 해쉬(Hash) 값을 붙여주는 것도 하나의 방법이다. 즉, 공격자가 원래 데이터를 임의 변조했을 때 비밀키 K를 모르는 공격자가 변형된 데이터의 인증 값을 만들 수 없게 함으로써 원래 데이터를 임의 변조할 수 없게 하는 것이다. 물론, 블록 암호화 알고리즘에서도 변경 방지를 위해 인증 값을 추가할 수 있다.

[0013] 하지만, 경우에 따라서는 이러한 인증 값을 만드는 것이 득보다 실이 되어 불필요한 경우가 있을 수 있다. 예컨대, 고화질의 비압축 데이터의 경우 수 Gbps의 매우 빠른 속도로 데이터를 보내야 하기 때문에 송/수신 에러가 발생했을 경우 에러가 완전히 보정되지 않아도 얼마간의 보정 작업을 거쳐 그냥 사용하는 것이 더 좋을 수 있는데, 데이터 인증값이 사용되게 될 경우 1비트의 에러가 발생하더라도 전체 데이터를 포기해야 하는 일이 발생할 수 있다.

[0014] 반대로, 압축된 데이터의 경우 컨텐츠 내부에 복사제어 정보 같은 중요 정보들이 있을 수 있다. 이때, 복사제어 정보의 설정이 '복사 금지(copy never)'로 되어있을 수 있는데, 데이터 인증 값이 없다면 해당 비트를 쉽게 변조할 수 있게 된다.

[0015] 이와 같이 종래 기술은 데이터의 종류에 상관없이 모든 데이터에 대하여 인증 값을 삽입하거나, 모든 데이터에 대하여 인증 값을 삽입하지 않는 방식을 이용하여, 데이터에 대하여 효율적으로 인증을 수행하지 못하는 문제점이 있었다.

발명이 이루고자 하는 기술적 과제

[0016] 본 발명의 목적은 데이터에 대한 효율적인 인증을 수행하기 위한 조건부 인증 코드 삽입 방법 및 그 장치, 인증을 통한 조건부 데이터 사용 방법 및 그 장치를 제공하는 것이다.

발명의 구성 및 작용

[0017] 상기 목적을 달성하기 위한 본 발명에 따른 조건부 인증 코드 삽입 방법은 데이터 패킷의 중요도 및 종류 중 적어도 하나에 따라 상기 데이터 패킷에 상기 데이터 패킷이 변조된 것인지 여부를 판단하기 위한 인증 코드를 삽입할 것인지 여부를 결정하는 단계; 및 상기 결정에 기초하여, 상기 인증 코드를 상기 데이터 패킷에 선택적으로 삽입하는 단계를 포함한다.

[0018] 바람직하게는 상기 결정하는 단계는 상기 데이터 패킷의 중요도 또는 상기 데이터 패킷의 종류 중 적어도 하나에 따라 상기 패킷에 상기 인증 코드를 삽입할 것인지 여부에 대한 정보 또는 상기 삽입 여부에 대한 판단 기준을 저장하고 있는 데이터베이스에 기초하여 상기 삽입 여부를 결정하는 것을 특징으로 한다.

[0019] 바람직하게는 상기 데이터 패킷은 상기 패킷의 헤더가 상기 데이터 패킷이 상기 인증 코드가 삽입된 패킷인지를 표시하는 인증 코드 삽입 표시 영역을 포함한다.

[0020] 바람직하게는 상기 인증 코드 삽입 표시 영역이 포함된 상기 패킷의 헤더를 이용하여 암호화 키를 생성하고, 상기 생성된 암호화 키를 이용하여 상기 데이터 패킷을 암호화하는 단계를 더 포함한다.

[0021] 바람직하게는 본 발명에 따른 조건부 인증 코드 삽입 방법은 상기 데이터 패킷이 인증 코드가 삽입된 패킷인지 여부에 따라 서로 다른 암호화 알고리즘을 이용하여 상기 데이터 패킷을 암호화하는 단계를 더 포함한다.

[0022] 바람직하게는 상기 결정하는 단계는 상기 데이터 패킷의 중요도가 높게 설정된 경우에는 상기 데이터 패킷에 상기 인증 코드를 삽입하고, 그 외의 경우에는 상기 데이터 패킷에 상기 인증 코드를 삽입하지 않도록 결정하는 것을 특징으로 한다.

[0023] 바람직하게는 상기 결정하는 단계는 상기 데이터 패킷이 압축된 데이터인 경우에는 상기 인증 코드를 삽입하고, 상기 데이터 패킷이 비압축 데이터인 경우에는 상기 데이터 패킷에 상기 인증 코드를 삽입하지 않도록 결정하는 것을 특징으로 한다.

[0024] 바람직하게는 상기 인증 코드는 CRC(cyclic redundancy checking)코드로 구성되는 것을 특징으로 한다.

[0025] 바람직하게는 상기 인증 코드는 HASH 함수를 이용하여 생성된 인증 코드로 구성되는 것을 특징으로 한다.

[0026] 또한, 상기 목적을 달성하기 위한 본 발명에 따른 인증을 통한 조건부 데이터 사용 방법은 데이터 패킷을 수신하고, 상기 수신된 데이터 패킷에 상기 데이터 패킷이 변조된 것인지 여부를 판단하기 위한 인증 코드가 삽입되었는지 여부를 판단하는 단계; 상기 판단결과에 기초하여, 상기 데이터 패킷에 대하여 선택적으로 변조 여부에 대한 인증을 수행하는 단계; 및 상기 인증 수행 여부 및 상기 인증 수행 결과에 기초하여, 상기 데이터 패킷을 선택적으로 사용하는 단계를 포함한다.

[0027] 바람직하게는 상기 판단하는 단계는 상기 데이터 패킷의 중요도 및 상기 데이터 패킷의 종류 중 적어도 하나에 따라 상기 패킷에 상기 인증 코드를 삽입할 것인지 여부에 대한 정보 또는 상기 삽입 여부에 대한 판단 기준을 저장하고 있는 데이터베이스에 기초하여 상기 삽입 여부를 판단한다.

[0028] 바람직하게는 상기 판단하는 단계는 상기 데이터 패킷이 상기 인증 코드가 삽입된 패킷인지를 표시하는 상기 패킷의 헤더의 인증 코드 삽입 표시 영역에 기초하여 상기 삽입 여부를 판단하는 것을 특징으로 한다.

[0029] 바람직하게는 상기 판단하는 단계는 상기 데이터 패킷을 암호화한 알고리즘의 종류에 따라 상기 삽입 여부를 판단하는 것을 특징으로 한다.

[0030] 바람직하게는 본 발명에 따른 인증을 통한 조건부 데이터 사용 방법은 상기 수신된 데이터 패킷에 에러가 있는 경우에는 상기 에러가 있는 데이터 패킷을 재수신하는 단계를 더 포함한다.

[0031] 바람직하게는 상기 재수신하는 단계는 상기 데이터 패킷에 상기 인증 코드가 삽입되었는지 여부에 따라 상기 재수신 횟수를 달리하여 상기 데이터 패킷을 재수신하는 것을 특징으로 한다.

[0032] 바람직하게는 상기 인증을 수행하는 단계는 상기 데이터 패킷에 상기 인증 코드가 삽입되었다고 판단되는 경우에는 상기 인증을 수행하고, 상기 데이터 패킷에 상기 인증 코드가 삽입되지 않았다고 판단되는 경우에는 상기 인증을 수행하지 않는 것을 특징으로 한다.

[0033] 바람직하게는 상기 데이터 패킷을 선택적으로 사용하는 단계는 상기 인증이 수행되지 않은 데이터 패킷 및 상기 인증 수행 결과 변조되지 않았다고 판단된 데이터 패킷은 사용하고, 그외의 데이터 패킷은 사용하지 않는 것을 특징으로 한다.

[0034] 또한, 상기 목적을 달성하기 위한 본 발명에 따른 조건부 인증 코드 삽입 장치는 데이터 패킷의 중요도 및 종류 중 적어도 하나에 따라 상기 데이터 패킷에 상기 데이터 패킷이 변조된 것인지 여부를 판단하기 위한 인증 코드를 삽입할 것인지 여부를 결정하는 인증 코드 삽입 결정부; 및 상기 결정에 기초하여, 상기 인증 코드를 상기 데이터 패킷에 선택적으로 삽입하는 인증 코드 삽입부를 포함한다.

[0035] 바람직하게는 본 발명에 따른 조건부 인증 코드 삽입 장치는 상기 인증 코드 삽입 표시 영역이 포함된 상기 패킷의 헤더를 이용하여 암호화 키를 생성하고, 상기 생성된 암호화 키를 이용하여 상기 데이터 패킷을 암호화하는 암호화부를 더 포함한다.

[0036] 또한, 상기 목적을 달성하기 위한 본 발명에 따른 인증을 통한 조건부 데이터 사용 장치는 데이터 패킷

을 수신하는 수신부; 상기 수신된 데이터 패킷에 상기 데이터 패킷이 변조된 것인지 여부를 판단하기 위한 인증 코드가 삽입되었는지 여부를 판단하는 인증 코드 삽입 판단부; 상기 판단결과에 기초하여, 상기 데이터 패킷에 대하여 선택적으로 변조 여부에 대한 인증을 수행하는 인증부; 및 상기 인증 수행 여부 및 상기 인증 수행 결과에 기초하여, 상기 데이터 패킷을 선택적으로 사용하는 데이터 사용부를 포함한다. .

[0037] 바람직하게는 본 발명에 따른 인증을 통한 조건부 데이터 사용 장치는 상기 수신된 데이터 패킷에 에러가 있는지를 검출하는 데이터 에러 검출부를 더 포함하고, 상기 수신부는 상기 수신된 데이터 패킷에 에러가 있는 경우에는 상기 에러가 있는 데이터 패킷을 재수신하는 것을 특징으로 하는 데이터 사용 장치.

[0038] 또한, 본 발명은 상기 목적을 달성하기 위하여 데이터 패킷의 중요도 및 종류 중 적어도 하나에 따라 상기 데이터 패킷에 상기 데이터 패킷이 변조된 것인지 여부를 판단하기 위한 인증 코드를 삽입할 것인지 여부를 결정하는 단계; 및 상기 결정에 기초하여, 상기 인증 코드를 상기 데이터 패킷에 선택적으로 삽입하는 단계를 포함하는 조건부 인증 코드 삽입 방법을 실행시키기 위한 프로그램이 기록된 컴퓨터로 읽을 수 있는 기록 매체를 제공한다.

[0039] 또한, 본 발명은 데이터 패킷을 수신하고, 상기 수신된 데이터 패킷에 상기 데이터 패킷이 변조된 것인지 여부를 판단하기 위한 인증 코드가 삽입되었는지 여부를 판단하는 단계; 상기 판단결과에 기초하여, 상기 데이터 패킷이 변조되었는지에 대하여 선택적으로 인증을 수행하는 단계; 및 상기 인증 수행 여부 및 상기 인증 수행결과에 기초하여, 상기 데이터 패킷을 선택적으로 사용하는 단계를 포함하는 인증을 통한 조건부 데이터 사용 방법을 실행시키기 위한 프로그램이 기록된 컴퓨터로 읽을 수 있는 기록 매체를 제공한다.

[0040] 이하에서는 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 대하여 상세히 설명한다.

[0041] 도 1은 본 발명에 따른 조건부 인증 코드 삽입 장치의 일실시예를 도시한 도면이다.

[0042] 도 1을 참조하면, 본 발명에 따른 조건부 인증 코드 삽입 장치는 인증 코드 삽입 결정부(110), 인증 코드 삽입부(120) 및 암호화부(130)를 포함한다.

[0043] 인증 코드 삽입 결정부(110)는 데이터 패킷의 중요도 및 종류 중 적어도 하나에 따라 데이터 패킷에 데이터 패킷이 변조된 것인지 여부를 판단하기 위한 인증 코드를 삽입할 것인지 여부를 결정한다.

[0044] 이때, 인증 코드란 데이터 패킷이 변조된 것인지 여부를 판단하기 위한 코드를 말하며, 이와 같은 인증 코드는 비밀 키로 암호화된 CRC(cyclic redundancy checking)코드로 구성될 수도 있고, 또는 비밀 키로 암호화된 HASH 또는 MAC 함수를 이용하여 생성된 인증 코드로 구성될 수도 있다. 이외에도 다양한 방식의 인증코드 생성 방식이 적용될 수 있다. 이와 같이 비밀 키로 암호화된 데이터를 인증 코드로 사용하는 이유는 제3자가 인증 코드를 변조하는 것을 방지하기 위함이다.

[0045] 한편, 인증 코드 삽입 결정부(110)는 데이터 패킷의 중요도가 높게 설정된 경우에는 데이터 패킷에 인증 코드를 삽입하고, 그 외의 경우에는 데이터 패킷에 인증 코드를 삽입하지 않도록 결정할 수 있다.

[0046] 또한, 인증 코드 삽입 결정부(110)는 데이터 패킷이 압축된 데이터 패킷인 경우에는 인증 코드를 삽입하고, 데이터 패킷이 비압축 데이터 패킷인 경우에는 데이터 패킷에 인증 코드를 삽입하지 않도록 결정할 수도 있다.

[0047] 이와 같이 비압축 데이터 패킷에 인증 코드를 삽입하지 않는 이유는, 예컨대 AV 비압축 데이터 패킷인 경우에 데이터 패킷의 일부가 변조되었다는 이유로 그 데이터 패킷을 사용하지 않게 되면, 일시적으로 화면에 아무런 영상을 출력할 수 없게 되는데, 이와 같이 화면에 어떤 영상도 출력하지 않는 것보다는, 설사 데이터 패킷의 일부가 변조되더라도 그 일부가 변조된 영상을 화면에 출력하는 것이 합리적이기 때문이다.

[0048] 이때, 인증 코드 삽입 결정부(110)는 데이터 패킷의 중요도 또는 데이터 패킷의 종류 중 적어도 하나에 따라 데이터 패킷에 인증 코드를 삽입할 것인지 여부에 대한 정보 또는 삽입 여부에 대한 판단 기준을 저장하고 있는 데이터베이스에 기초하여 인증 코드의 삽입 여부를 결정할 수도 있다.

[0049] 이와 같은 데이터베이스에는 사용자가 설정한 기준에 따라 인증 코드를 삽입하기 위한 데이터 패킷의 중요도 및 종류가 결정되어 있으며, 그 기준은 사용자의 선택에 의하여 수시로 변경될 수 있다.

[0050] 한편, 사용자가 데이터 패킷의 중요도 및 종류를 직접 확인하여, 인증 코드를 삽입할 것인지 여부를 결

정할 수도 있다. 이와 같이 인증 코드 삽입여부 판단이 필요 없는 경우에는 인증 코드 삽입 결정부(110)가 생략될 수도 있다.

[0051] 인증 코드 삽입부(120)는 인증 코드 삽입 결정부(100)의 결정에 기초하여, 인증 코드를 데이터 패킷에 선택적으로 삽입한다.

[0052] 인증 코드 삽입부(120)에 의하여 인증 코드가 삽입된 데이터 패킷은 수학식 2와 같이 표시될 수 있다.

[0053] [수학식 2]

[0054] $$데이터||인증코드$$

[0055] 전술한바와 같이, 이때의 인증 코드는 비밀 키로 암호화된 CRC(cyclic redundancy checking)코드로 구성될 수도 있고, 또는 비밀키로 암호화된 HASH 또는 MAC 함수를 이용하여 생성된 인증 코드로 구성될 수도 있다.

[0056] 이때, 본 실시예의 데이터 패킷은 그 데이터 패킷의 헤더에 인증 코드가 삽입된 데이터 패킷인지 여부를 표시하는 인증 코드 삽입 표시 영역을 포함할 수 있다.

[0057] 예컨대, 인증 코드 삽입부(120)는 데이터 패킷에 인증 코드가 삽입된 경우에는 데이터 패킷의 헤더에 포함된 인증 코드 삽입 표시 영역에 1을 표시하고, 인증 코드가 삽입되지 않은 데이터 패킷인 경우에는 인증 코드 삽입 표시 영역에 0을 표시할 수도 있다.

[0058] 또한, 인증 코드 삽입부(120)는 데이터 패킷에 인증 코드가 삽입된 경우에는 데이터 패킷에 임의의 표시를 하거나, 소정의 데이터를 더 부가하는 방식으로 그 삽입 사실을 표시하고, 데이터 패킷에 인증 코드가 삽입되지 않은 경우에는 아무런 표시를 하지 않을 수도 있다.

[0059] 암호화부(130)는 인증 코드 삽입 표시 영역이 포함된 데이터 패킷의 헤더를 이용하여 암호화 키를 생성하고, 그 생성된 암호화 키를 이용하여 데이터 패킷을 암호화한다.

[0060] 이와 같이 암호화부(130)에서 인증 코드 삽입 표시 영역이 포함된 데이터 패킷의 헤더를 이용하여 암호화 키를 생성하고, 그 암호화 키를 이용하여 데이터 패킷을 암호화하는 이유는, 인증 코드 삽입 표시 영역의 표시가 제3자에 의하여 변조되는 것을 방지하기 위한 것이다.

[0061] 즉, 수신측에서 데이터 패킷의 헤더를 이용하여 복호화 키를 생성하고, 그 생성된 복호화 키를 이용하여 암호화된 데이터 패킷을 복호화하는 경우에, 데이터 패킷의 헤더의 인증 코드 삽입 표시 영역이 변조된 경우에는 암호화 키와 복호화 키가 달라져서, 그 암호화된 데이터를 복호화할 수 없게 되어 그 데이터 패킷의 헤더가 변조되었음을 알 수 있게 되는 것이다. 이때, 데이터 패킷의 헤더는 복호화 키 생성을 위한 정보가 되므로 암호화되지 않은 채로 수신측에 전송된다.

[0062] 이와 같은 과정을 통해, 수신측에서는 제3자가 데이터 패킷의 인증 코드 삽입 표시 영역의 표시를 변조하는 것을 방지할 수 있다.

[0063] 다만, 인증 코드 삽입 표시 영역의 표시가 변조되는 것을 방지하기 위한 방법은 이와 같은 암호화 방법에 한정되지 않는다.

[0064] 또한, 암호화부(130)는 데이터 패킷이 인증 코드가 삽입된 데이터 패킷인지 여부에 따라 서로 다른 암호화 알고리즘을 이용하여 데이터 패킷을 암호화할 수 있다.

[0065] 예컨대, 인증 코드가 삽입된 데이터 패킷인 경우에는 AES(Advanced Encryption Standard) CBC 모드 알고리즘을 이용하여 암호화하고, 인증 코드가 삽입되지 않은 데이터 패킷인 경우에는 AES 카운터 모드 알고리즘을 이용하여 암호화할 수 있다.

[0066] 이와 같이, 인증 코드의 삽입여부에 따라 암호화 알고리즘을 달리하여 암호화하는 이유는, 수신측에서 암호화 알고리즘에 따라 수신된 데이터 패킷이 인증 코드가 삽입된 데이터 패킷인지 여부를 미리 판단할 수 있게 하기 위함이다.

[0067] 즉, 상기 예에서 수신측은 AES CBC 모드 알고리즘을 이용하여 암호화된 데이터 패킷은 인증 코드가 삽입된 데이터 패킷이고, AES 카운터 모드 알고리즘을 이용하여 암호화된 데이터 패킷은 인증 코드가 삽입되지 않

은 데이터 패킷으로 판단할 수 있는 것이다.

[0068] 다만, 이때 사용되는 암호화 알고리즘은 AES CBC 모드 알고리즘 및 AES 카운터 모드 알고리즘에 한정되지 않고, 다른 암호화 알고리즘이 사용될 수 있다.

[0069] 또한, 암호화부(130)는 구현예에 따라서 생략될 수도 있다.

[0070] 도 2는 본 발명에 따른 조건부 인증 코드 삽입 방법의 일실시예를 설명하기 위하여 도시한 흐름도이다.

[0071] 단계 210에서는, 데이터 패킷의 중요도 및 종류에 따라 데이터 패킷에 데이터 패킷이 변조된 것인지 여부를 판단하기 위한 인증 코드를 삽입할 것인지 여부를 결정한다.

[0072] 단계 220에서는, 삽입 여부에 대한 결정에 기초하여, 인증 코드를 데이터 패킷에 선택적으로 삽입한다.

[0073] 단계 230에서는, 인증 코드 삽입 표시 영역이 포함된 데이터 패킷의 헤더를 이용하여 암호화 키를 생성하고, 생성된 암호화 키를 이용하여 데이터 패킷을 암호화한다.

[0074] 이때, 인증 코드 삽입 표시 영역의 표시의 변조를 방지할 수 있는 다른 방법이 있는 경우에는 단계 230은 그 변조 방지를 위한 방법으로 대체될 수 있다. 또한 단계 220과 단계 230은 인증 방식에 따라 그 순서가 바뀔 수 있다. 즉, 데이터 패킷 암호화 후에 인증 코드를 붙일 수도 있다.

[0075] 도 3은 본 발명에 따른 인증을 통한 조건부 데이터 사용 장치의 일 실시예를 설명하기 위하여 도시한 도면이다.

[0076] 도 3을 참조하면, 본 발명에 따른 인증을 통한 조건부 데이터 사용 장치는 수신부(310), 인증 코드 삽입 판단부(320), 인증부(330), 에러 검출부(340) 및 데이터 사용부(350)를 포함한다.

[0077] 수신부(310)는 데이터 패킷을 수신한다.

[0078] 이때, 데이터 패킷은 암호화된 데이터 패킷일 수도 있고, 암호화되지 않은 데이터 패킷일 수도 있다.

[0079] 인증 코드 삽입 판단부(320)는 수신된 데이터 패킷에 데이터 패킷이 변조된 것인지 여부를 판단하기 위한 인증 코드가 삽입되었는지 여부를 판단한다.

[0080] 이때, 인증 코드 삽입 판단부(320)는 데이터 패킷의 중요도 및 데이터 패킷의 종류 중 적어도 하나에 따라 데이터 패킷에 인증 코드를 삽입할 것인지 여부에 대한 정보 또는 삽입 여부에 대한 판단 기준을 저장하고 있는 데이터베이스에 기초하여 삽입 여부를 판단할 수 있다.

[0081] 예컨대, 인증 코드 삽입 판단부(320)는 데이터베이스에 비압축 데이터 패킷이 인증 코드가 삽입되어야 할 데이터 패킷이 아니라고 결정되어 있는 경우에는, 수신된 데이터 패킷이 비압축 데이터 패킷인 것으로 판단되기만 하면 인증 코드가 삽입되지 않았다고 판단하게 되는 것이다.

[0082] 또한, 인증 코드 삽입 판단부(320)는 데이터 패킷이 인증 코드가 삽입된 데이터 패킷인지를 표시하는 데이터 패킷의 헤더의 인증 코드 삽입 표시 영역에 기초하여 삽입 여부를 판단할 수 있다.

[0083] 예컨대, 수신된 데이터 패킷의 헤더의 인증 코드 삽입 표시 영역에 1이 표시된 경우에는 그 데이터 패킷은 인증 코드가 삽입된 데이터 패킷으로 판단하고, 인증 코드 삽입 표시 영역에 0이 표시된 경우에는 인증 코드가 삽입되지 않은 데이터 패킷으로 판단할 수 있다.

[0084] 또한, 인증 코드 삽입 판단부(320)는 수신된 데이터 패킷을 암호화한 알고리즘의 종류에 따라 인증 코드의 삽입 여부를 판단할 수도 있다.

[0085] 이 경우에는 인증 코드 삽입 판단부(320)는 암호화된 데이터를 복호화하기 위한 복호화부(미도시)를 더 포함할 수 있다.

[0086] 즉, 이 경우에 수신된 데이터 패킷이 복호화부를 통하여 AES(Advanced Encryption Standard) CBC 모드 알고리즘을 이용하여 복호화가 가능한 경우에는 인증 코드가 삽입된 데이터 패킷으로 판단하고, AES 카운터 모드 알고리즘을 이용하여 복호화가 가능한 경우에는 인증 코드가 삽입되지 않은 데이터 패킷으로 판단할 수 있다.

[0087] 인증부(340)는 인증 코드 삽입 판단부(320)의 판단결과에 기초하여, 데이터 패킷에 대하여 선택적으로 변조 여부에 대한 인증을 수행한다.

[0088] 즉, 인증부(340)는 데이터 패킷에 인증 코드가 삽입되었다고 판단되는 경우에는 인증을 수행하고, 데이터 패킷에 인증 코드가 삽입되지 않았다고 판단되는 경우에는 인증을 수행하지 않을 수 있다.

[0089] 에러 검출부(330)는 수신부(310)로부터 수신된 데이터 패킷에 에러가 있는지를 검출한다.

[0090] 수신부(310)는 에러 검출부(330)의 검출결과, 수신된 데이터 패킷에서 에러검출된 경우에는 에러가 있는 데이터 패킷을 재수신하게 된다.

[0091] 이때, 수신부(310)는 데이터 패킷에 인증 코드가 삽입되었는지 여부에 따라 재수신 횟수를 달리하여 데이터 패킷을 재수신하게 된다.

[0092] 즉, 수신부(310)는 에러 검출부(330)에 의하여 수신된 데이터 패킷에서 에러가 검출되었다는 것이 인지되면, 인증 코드 삽입 판단부(320)의 판단 결과에 따라 에러가 검출된 데이터 패킷이 인증 코드가 삽입된 데이터 패킷인지를 판단하여 에러가 발생한 데이터 패킷의 재수신 횟수를 결정하는 것이다.

[0093] 예컨대, 에러가 검출된 데이터 패킷이 인증 코드가 삽입된 중요한 데이터 패킷이라고 판단되면, 에러가 검출되지 않은 데이터 패킷을 수신할 때까지 10회까지 재수신할 수 있지만, 인증 코드가 삽입되지 않은 비압축 AV 데이터라고 판단되는 경우에는 그 에러가 발생한 데이터 패킷을 재수신하지 않고, 에러가 발생한 데이터 패킷을 그대로 사용할 수도 있는 것이다.

[0094] 데이터 사용부(350)는 인증 수행 여부 및 인증 수행 결과에 기초하여, 데이터 패킷을 선택적으로 사용한다.

[0095] 데이터 사용부(350)는 인증이 수행되지 않은 데이터 패킷 및 인증 수행 결과 변조되지 않았다고 판단된 데이터 패킷은 사용하고, 그외의 데이터 패킷은 사용하지 않는다.

[0096] 즉, 인증이 수행되지 않은 데이터 패킷은 인증이 필요없는 것이므로 변조되었는지 여부에 대한 판단 없이 사용하게 되는 것이고, 인증이 수행된 데이터 패킷은 변조되지 않았다고 판단되는 데이터 패킷에 한하여 사용하는 것이다.

[0097] 이때, 사용이란 데이터 패킷이 영상인 경우에 화면에 출력하는 것일 수도 있고, 수신된 데이터 패킷이 오디오인 경우에는 그 오디오 파일을 재생하는 것일 수 있다. 또한, 데이터 패킷이 일반 데이터 파일인 경우에는 저장하는 것일 수도 있다.

[0098] 도 4는 본 발명에 따른 인증을 통한 조건부 데이터 사용 방법의 일실시예를 설명하기 위하여 도시한 흐름도이다.

[0099] 단계 410에서는, 데이터 패킷을 수신한다.

[0100] 단계 420에서는, 수신된 데이터 패킷에 데이터 패킷이 변조된 것인지 여부를 판단하기 위한 인증 코드가 삽입되었는지 여부를 판단한다.

[0101] 단계 430에서는, 인증 코드가 삽입된 데이터 패킷에 대하여 데이터 패킷이 변조되었는지 여부에 대한 인증을 수행한다.

[0102] 단계 440에서는, 데이터 패킷에 대한 인증이 수행되지 않은 패킷 및 인증 수행 결과 변조되지 않았다고 판단된 데이터 패킷을 사용한다.

[0103] 이때, 데이터 사용부(350)는 인증 수행 결과 변조되었다고 판단된 데이터 패킷은 사용하지 않는다.

[0104] 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.

[0105] 상기 컴퓨터로 읽을 수 있는 기록매체는 마그네틱 저장매체(예를 들면, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등) 및 캐리어 웨이브(예를 들면, 인터넷을 통한 전송)와 같은 저장매체를 포함한다.

[0106] 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 구현될 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 범

위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

발명의 효과

[0107] 본 발명은 데이터 패킷의 중요도 및 종류 중 적어도 하나에 따라 데이터 패킷에 데이터 패킷이 변조된 것인지 여부를 판단하기 위한 인증 코드를 삽입할 것인지 여부를 결정하고, 그 결정에 기초하여, 인증 코드를 데이터 패킷에 선택적으로 삽입함으로써, 데이터에 대한 효율적인 인증을 수행할 수 있는 효과가 있다.

도면의 간단한 설명

[0001] 도 1은 본 발명에 따른 조건부 인증 코드 삽입 장치의 일실시예를 도시한 도면이다.

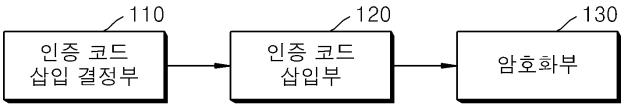
[0002] 도 2는 본 발명에 따른 조건부 인증 코드 삽입 방법의 일실시예를 설명하기 위하여 도시한 흐름도이다.

[0003] 도 3은 본 발명에 따른 인증을 통한 조건부 데이터 사용 장치의 일 실시예를 설명하기 위하여 도시한 도면이다.

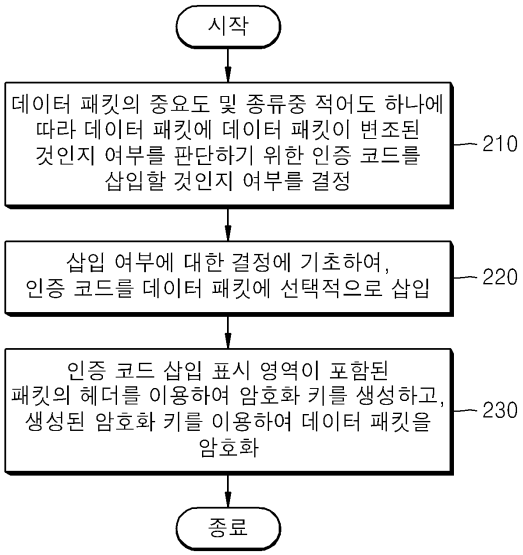
[0004] 도 4는 본 발명에 따른 인증을 통한 조건부 데이터 사용 방법의 일실시예를 설명하기 위하여 도시한 흐름도이다.

도면

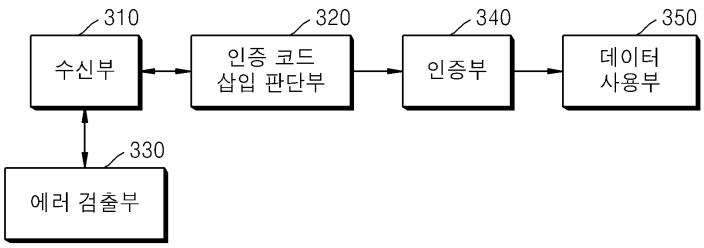
도면1



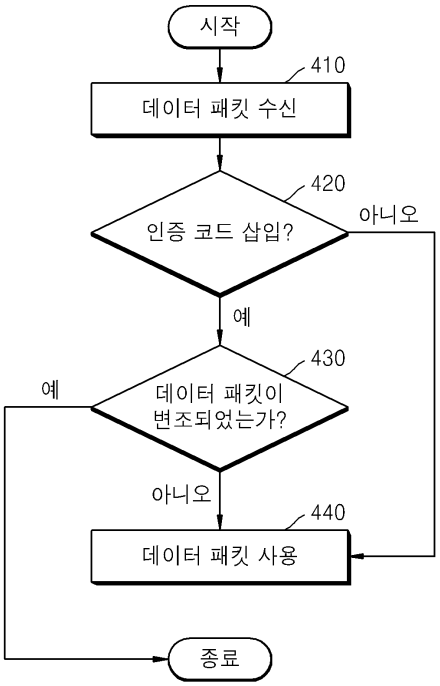
도면2



도면3


310
수신부
320
인증 코드
삽입 판단부
340
인증부
350
데이터
사용부
330
에러 검출부

도면4


시작
410
데이터 패킷 수신
420
인증 코드 삽입?
아니오
예
430
데이터 패킷이
변조되었는가?
예
아니오
440
데이터 패킷 사용
종료