(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년03월18일
(11) 등록번호 10-1375670
(24) 등록일자 2014년03월12일

(51) 국제특허분류(Int. Cl.)
H04L 9/18 (2006.01) *H04L 9/28* (2006.01)
(21) 출원번호 10-2007-0044700
(22) 출원일자 2007년05월08일
심사청구일자 2012년04월06일
(65) 공개번호 10-2008-0099071
(43) 공개일자 2008년11월12일
(56) 선행기술조사문헌
Kungl Tekniska Hogskolan Stockholm Master of Science Thesis, "Key Agreement for Secure Voice Over IP" (December 2003)
JP2005510184 A*
US20050213751 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
이형직
경기도 성남시 분당구 수내로 74, 116동 703호 (수내동, 양지마을)
신준범
경기도 수원시 영통구 봉영로 1526, 살구골7단지 아파트 717동 104호 (영통동)
(뒷면에 계속)
(74) 대리인
리앤목특허법인

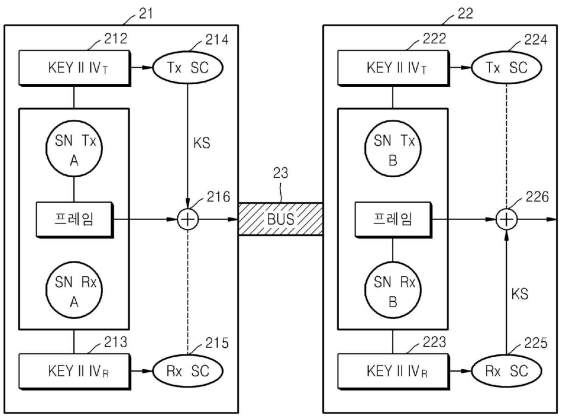
전체 청구항 수 : 총 5 항 심사관 : 이병수

(54) 발명의 명칭 **데이터의 암호화/복호화 방법 및 이를 적용한 버스 시스템**

(57) 요 약

본 발명은 암호화 방법에 관한 것으로, 데이터를 포함하는 바디 및 헤더로 구성된 프레임 단위로 데이터를 전송하는 경우 소정의 키(key)와 초기화 벡터를 기초로 생성된 키 스트림과 바디에 포함된 데이터를 연산함으로써 암호화된 데이터를 버스로 전송하고, 프레임의 전송 순서를 나타내는 순서 번호(sequence number)를 포함하는 헤더를 버스로 전송함으로써, 기존의 버스 시스템에 대한 수정 없이 버스에서 전송되는 데이터에 대한 보안을 강화할 수 있다.

대 표 도 - 도2



(72) 발명자

최양림

경기도 성남시 분당구 미금로 184, - 103동 704호 (구미동, 까치마을)

김진목

경기도 용인시 기흥구 이현로29번길 86-13, 111동 501호 (보정동, 대림아파트)

특허청구의 범위

청구항 1

데이터를 포함하는 바디 및 헤더로 구성된 프레임 단위로 전송되는 상기 데이터의 암호화 방법에 있어서,

소정의 키(key)와 초기화 벡터를 기초로 생성된 키 스트림과 상기 바디에 포함된 데이터를 연산함으로써 암호화된 데이터를 버스로 전송하는 단계;

상기 프레임의 전송 순서를 나타내는 순서 번호(sequence number)를 포함하는 상기 헤더를 상기 버스로 전송하는 단계; 및

상기 초기화 벡터가 갱신되는 경우 상기 초기화 벡터를 상기 바디에 포함시키고, 상기 바디를 포함하는 제어 프레임을 상기 버스로 전송하는 단계를 포함하는 것을 특징으로 하는 데이터 암호화 방법.

청구항 2

제1항에 있어서,

상기 초기화 벡터가 갱신되는 경우 상기 초기화 벡터를 상기 바디에 포함시키고,

상기 키 스트림과 상기 초기화 벡터를 연산하여 상기 초기화 벡터를 암호화하는 단계를 더 포함하는 것을 특징으로 하는 데이터 암호화 방법.

청구항 3

데이터를 포함하는 바디 및 헤더로 구성된 프레임 단위로 전송되는 상기 데이터의 복호화 방법에 있어서,

상기 헤더로부터 추출된 발신용 순서 번호를 수신 모듈의 수신용 순서 번호와 비교하는 단계; 및

비교 결과 상기 발신용 순서 번호와 상기 수신용 순서 번호가 일치하는 경우 소정의 키와 초기화 벡터를 기초로 생성된 키 스트림과 상기 바디에 포함된 데이터를 연산함으로써 상기 데이터를 복호화하는 단계를 포함하고,

상기 초기화 벡터가 갱신되는 경우, 갱신된 초기화 벡터가 포함된 제어 프레임이 수신되어 상기 초기화 벡터가 갱신되는 것을 특징으로 하는 데이터 복호화 방법.

청구항 4

제3항에 있어서,

상기 발신용 순서 번호와 상기 수신용 순서 번호가 불일치하는 경우

상기 초기화 벡터를 갱신하고, 갱신된 초기화 벡터를 상기 프레임을 전송한 모듈로 전송하는 단계를 더 포함하는 것을 특징으로 하는 데이터 복호화 방법.

청구항 5

버스로 연결된 제1 및 제2 모듈이 데이터를 포함하는 바디 및 헤더로 구성된 프레임 단위로 상기 데이터를 송수신하는 버스 시스템에 있어서,

상기 제1 및 제2 모듈은 각각

발신 프레임의 헤더에 상기 발신 프레임의 전송 순서를 나타내는 순서 번호를 기록하고, 수신 프레임의 헤더를 파싱하는 프레임 핸들러;

상기 발신 프레임의 바디에 포함된 데이터를 암호화하는 스트림 암호화 송신부; 및

상기 수신 프레임의 헤더에 포함된 순서 번호가 수신하고자 하는 프레임의 순서 번호와 일치하는 경우 상기 수신 프레임의 바디에 포함된 데이터를 복호화하는 스트림 암호화 수신부를 포함하고,

초기화 벡터가 갱신되는 경우, 갱신된 초기화 벡터가 포함된 제어 프레임이 수신되어 상기 초기화 벡터가 갱신되는 것을 특징으로 하는 버스 시스템.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0010] 본 발명은 암호화 방법에 관한 것으로, 더욱 상세하게는 데이터의 암호화(encryption) 및 복호화(decryption) 방법, 및 버스 시스템에 관한 것이다.

[0011] 암호 시스템은 키(key)를 운영하는 방식에 따라 공개키 암호 시스템과 비밀키 암호 시스템으로 나눌 수 있다. 공개키 암호 시스템에서 모든 사용자는 모든 사람에게 공개되어 있는 공개키(public key)와 자기만의 개인키(private key 또는 secret key)를 가지고 있으며, 공개키는 문서를 암호화할 때 사용하며 개인키는 개인이 보관을 하면서 암호화된 문서를 해독할 때 사용한다. 이에 반해, 비밀키 암호 시스템은 하나의 비밀키만으로 암호화 및 복호화(해독)를 동시에 수행하는 것으로, 블록 암호(block cipher) 시스템과 스트림 암호(stream cipher) 시스템이 있다.

[0012] 블록 암호 시스템은 주어진 평문(plain text)을 정해진 길이의 블록(64 비트 혹은 128 비트)으로 나누어 블록 단위로 암호화를 수행한다. 스트림 암호 시스템은 평문을 블록으로 나누지 않고, 비밀키로부터 유도된 키 스트림(key stream)과 평문에 대하여 배타적 논리합(XOR)을 수행하여 암호문을 생성한다. 일반적으로 스트림 암호 시스템은 블록 암호 시스템에 비해 속도가 빠르다.

[0013] 도 1은 종래의 스트림 암호 시스템을 나타내는 블록도이다.

[0014] 도 1을 참조하면, 스트림 암호 시스템은 CPU(central processing unit, 11), 캐쉬(cache, 12), 메모리 컨트롤러(memory controller, 13), 암호화/복호화부(encryption/decryption unit, 14), 연산부(15) 및 외부 메모리(external memory, 16)를 포함한다.

[0015] 먼저, CPU(11)에서 버스로 전송되는 데이터를 암호화하는 동작에 대하여 설명하기로 한다. CPU(11)에서 데이터에 대한 읽기/쓰기를 요청(request)하는 경우 생성되는 데이터는 암호화되지 않은 평문(plaintext) 데이터이므로, 이를 버스로 전송하기 위해서는 암호화하는 과정이 필요하다. CPU(11)가 데이터에 대한 읽기/쓰기를 요청하면, 암호화/복호화부(14)는 데이터에 대한 읽기/쓰기 요청을 탐지한다. 이 때, 암호화/복호화부(14)에 포함된 키 스트림 생성부(141)는 클럭 신호에 동기하여(즉, 클럭 신호의 상승 및/또는 하강 에지(edge)에서) 데이터의 사이즈에 해당하는 키 스트림을 발생한다. 여기서, 데이터의 사이즈는 예를 들어, 바이트 또는 입력된 데이터로부터 줄, 단어, 문자의 개수 등을 계산한 워드 카운트 등으로 나타낼 수 있다. 연산부(15)는 키 스트림과 데이터에 대하여 각각 바이트 단위로 일대일 매핑이 되도록 동기되어 배타적 논리합(XOR)을 수행하여 데이터를 암호화한다. 이와 같이, 암호화된 데이터는 버스를 통하여 외부로 전송될 수 있다.

[0016] 다음으로, 버스를 통해 전송되는 암호화된 데이터를 CPU(11)가 인식할 수 있도록 복호화하는 동작에 대하여 설명하기로 한다. 외부 메모리(16)로부터 버스를 통해 전송되는 암호화된 데이터는 메모리 컨트롤러(13) 및 캐쉬(12)를 거쳐서 CPU(11)로 전달되는데 CPU(11)는 암호화된 데이터를 인식할 수 없으므로 이를 복호화하는 과정이 필요하다. 외부 메모리(16)로부터 버스를 통해 암호화된 데이터가 전송되면, 암호화/복호화부(14)는 이를 탐지한다. 이 때, 암호화/복호화부(14)에 포함된 키 스트림 생성부(141)는 클럭 신호에 동기하여 키 스트림을 발생한다. 연산부(15)는 키 스트림과 암호화된 데이터에 대하여 각각 바이트 단위로 일대일 매핑이 되도록 동기되어 배타적 논리합을 수행하여 데이터를 복호화한다. 이와 같이, 복호화된 데이터는 CPU(11)에 입력된다.

[0017] 여기서, CPU(11), 캐쉬(12), 메모리 컨트롤러(13), 암호화/해독화부(14), 및 연산부(15)를 포함하는 영역은 신뢰 영역(trusted area)이라고 할 수 있으며, 신뢰 영역을 제외한 모든 모듈, 예를 들어, 외부 메모리(15)는 비신뢰 영역(non-trusted area)이라고 할 수 있다. 비신뢰 영역에서 버스를 통해 전송되는 데이터는 태핑(tapping) 등을 통하여 외부에 노출될 위험이 있다. 여기서, 태핑은 버스를 통해 전송되는 데이터를 다른 선을 통해 외부로 노출시키는 것을 말한다. SoC(system on chip)나 단일 칩 내부는 신뢰 영역으로 데이터가 보호될 수 있으나, 하나의 보드 상에 서로 다른 모듈을 붙여서 사용하는 경우에는 신뢰 영역으로 데이터가 보호받기 어렵다. 왜냐하면, 보드 상에서 버스를 통해 전송되는 데이터는 태핑을 통해 정보가 노출될 가능성이 있기 때문이다.

[0018] 또한, 종래의 스트림 암호 시스템은 하드웨어로 구현되므로 상당한 개발 기간이 소요되었으며, 활용 범위가 제한적이었다.

발명이 이루고자 하는 기술적 과제

[0019] 본 발명이 이루고자 하는 기술적 과제는 기존의 오픈 버스 시스템에서 하드웨어의 수정 없이 안전하게 데이터를 전송할 수 있는 데이터 암호화 방법을 제공하는데 있다. 본 발명이 이루고자 하는 다른 기술적 과제는 기존의 오픈 버스 시스템에서 하드웨어의 수정 없이 안전하게 데이터를 전송할 수 있는 데이터 복호화 방법을 제공하는데 있다. 본 발명이 이루고자 하는 또 다른 기술적 과제는 기존의 오픈 버스 시스템의 하드웨어의 수정 없이 안전하게 데이터를 전송할 수 있는 버스 시스템을 제공하는데 있다.

발명의 구성 및 작용

[0020] 상기 기술적 과제를 해결하기 위한 본 발명에 따른 데이터 암호화 방법은 데이터를 포함하는 바디 및 헤더로 구성된 프레임 단위로 데이터를 전송하는 경우 소정의 키(key)와 초기화 벡터를 기초로 생성된 키 스트림과 상기 바디에 포함된 데이터를 연산함으로써 암호화된 데이터를 버스로 전송하는 단계, 및 상기 프레임의 전송 순서를 나타내는 순서 번호(sequence number)를 포함하는 상기 헤더를 상기 버스로 전송하는 단계를 포함한다.

[0021] 또한, 상기 다른 기술적 과제를 해결하기 위한 본 발명에 따른 데이터 복호화 방법은 데이터를 포함하는 바디 및 헤더로 구성된 프레임 단위로 데이터가 전송되는 경우 상기 헤더로부터 추출된 발신용 순서 번호를 수신 모듈의 수신용 순서 번호와 비교하는 단계, 및 비교 결과 상기 발신용 순서 번화와 상기 수신용 순서 번호가 일치하는 경우 소정의 키와 초기화 벡터를 기초로 생성된 키 스트림과 상기 바디에 포함된 데이터를 연산함으로써 상기 데이터를 복호화하는 단계를 포함한다.

[0022] 또한, 상기 또 다른 기술적 과제를 해결하기 위한 본 발명에 따른 버스 시스템은 버스로 연결된 제1 및 제2 모듈이 데이터를 포함하는 바디 및 헤더로 구성된 프레임 단위로 상기 데이터를 송수신하며, 상기 제1 및 제2 모듈은 각각 발신 프레임의 헤더에 상기 발신 프레임의 전송 순서를 나타내는 순서 번호를 기록하고, 수신 프레임의 헤더를 파싱하는 프레임 핸들러, 상기 발신 프레임의 바디에 포함된 데이터를 암호화하는 스트림 암호화 송신부, 및 상기 수신 프레임의 헤더에 포함된 순서 번호가 수신하고자 하는 프레임의 순서 번호와 일치하는 경우 상기 수신 프레임의 바디에 포함된 데이터를 복호화하는 스트림 암호화 수신부를 포함한다.

[0023] 본문에 개시되어 있는 본 발명의 실시예들에 대해서, 특정한 구조적 내지 기능적 설명들은 단지 본 발명의 실시예를 설명하기 위한 목적으로 예시된 것으로, 본 발명의 실시예들은 다양한 형태로 실시될 수 있으며 본문에 설명된 실시예들에 한정되는 것으로 해석되어서는 아니 된다.

[0024] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 형태를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 본문에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 개시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 구성요소에 대해 사용하였다.

[0025] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0026] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.

[0027] 도 2는 본 발명의 일 실시예에 따른 버스 시스템을 나타내는 블록도이다.

[0028] 도 2를 참조하면, 버스 시스템은 제1 모듈(21) 및 제2 모듈(22)을 포함하고, 제1 및 제2 모듈(21, 22)은 버스(23)로 연결된다. 제1 모듈(21)은 제1 프레임 핸들러(frame handler, 211), 제1 및 제2 시드(seed) 생성부(212, 213), 제1 스트림 암호화 송신부(Tx SC, 214), 제1 스트림 암호화 수신부(Rx SC, 215) 및 제1 연산부(216)를 포함한다. 제2 모듈(22)은 제2 프레임 핸들러(221) 제3 및 제4 시드 생성부(222, 223), 제2 스트림 암호화 송신부(224), 제2 스트림 암호화 수신부(225) 및 제2 연산부(226)를 포함한다.

[0029] 제1 모듈(21)에서 생성된 데이터는 프레임의 단위로 제2 모듈(22)로 전송된다. 이하에서는 도 3 내지 도 6을 참조하여, 본 발명의 일 실시예에 따른 프레임의 구조 및 종류에 대하여 설명하고, 다시 도 2를 참조하여 본 발명의 일 실시예에 따른 버스 시스템의 구성 및 동작에 대하여 설명하기로 한다.

[0030] 도 3은 본 발명의 일 실시예에 따른 프레임의 구조를 나타내는 개략도이다.

[0031] 도 3을 참조하면, 일반적으로 데이터는 헤더(header) 및 바디(body)로 구성된 프레임(frame)의 형태로 버스를 통하여 전송된다. 바디는 페이로드(payload)와 동일하며, 이는 가공되지 않은 원래의 평문(plaintext) 데이터를 나타낸다. 바디에 포함된 평문 데이터는 암호화되어 버스로 전송된다. 헤더는 바디에 포함된 평문 데이터의 속성 정보 등을 나타낸다. 본 발명의 일 실시예에서 프레임은 헤더 및 바디를 포함한 32 비트로 구성할 수 있다. 그러나, 이는 본 발명의 일 실시예에 불과하며, 바디의 사이즈 및 프레임의 길이는 다양하게 변경할 수 있음은 당업자에게 자명하다.

[0032] 도 4는 도 3의 프레임에 포함된 헤더의 구조를 나타내는 개략도이다.

[0033] 도 4를 참조하면, 헤더는 순서 번호(sequence number) 및 명령어 식별자(command ID)를 포함할 수 있다. 본 발명의 일 실시예에서 순서 번호는 28 비트이고, 명령어 식별자는 4비트일 수 있고, 그 결과 순서 번호 및 명령어 식별자로 구성된 헤더는 32 비트일 수 있다.

[0034] 순서 번호는 데이터를 버스에 보낼 수 있도록 프레임으로 나눈 경우 그 순서에 따라 붙인 일련 번호를 나타낸다. 본 발명의 일 실시예에 따른 버스 시스템에 포함된 모듈은 송수신 순서에 따른 순서 번호를 가진다. 일반적으로, 전송이 시작될 때, 순서 번호는 0부터 시작되고, 전송되는 프레임의 수가 증가할수록 순서 번호도 1만큼 증가한다. 예를 들어, 순서 번호가 4비트인 경우, 첫 번째 프레임이 전송되는 경우의 순서 번호는 0000이고, 두 번째 프레임이 전송되는 경우의 순서 번호는 0001이며, 세 번째 프레임이 전송되는 경우의 순서 번호는 0010이다. 이와 같이, 순서 번호는 1씩 증가하며, 더 이상 증가할 수 없는 경우에는 다시 0000으로 된다.

[0035] 구체적으로, 데이터를 전송하는 제1 모듈은 프레임의 헤더에 송신용 순서 번호를 포함시키고, 이를 버스를 통해 제2 모듈로 전송한다. 이 경우 제2 모듈은 헤더로부터 송신용 순서 번호를 추출하여, 이를 제2 모듈에 해당하는 수신용 순서 번호와 비교한다. 비교 결과, 송신용 순서 번호와 수신용 순서 번호가 일치하는 경우에만 복호화 동작을 수행하여 데이터의 보안성을 향상시킬 수 있다.

[0036] 명령어 식별자는 바디에 포함된 데이터의 종류를 나타내고, 프레임을 수신하는 모듈은 헤더에서 명령어 식별자를 추출하여 프레임의 종류를 인식할 수 있다. 이하에서 도 5를 참조하여 명령어 식별자에 대하여 상술하기로 한다.

[0037] 도 5는 도 4의 헤더에 포함된 명령어 식별자를 나타내는 표이다.

[0038] 도 5를 참조하면, 본 발명의 일 실시예에서 명령어 식별자는 4비트로 표시되고, 명령어 식별자가 '0000'인 경우에는 바디에 데이터가 포함되어 암호화되었음을 나타낸다.

[0039] 명령어 식별자가 '0001'인 경우에는 바디에 새로운 초기화 벡터(initialization vector, IV)가 포함되어 암호화되었음을 나타낸다. 초기화 벡터는 암호화 알고리즘의 초기화에 이용되는 랜덤(random)한 이진 수로서, 소정의 키(key)와 함께 시드(seed)를 구성하여 키 스트림을 생성하는 기초가 된다. 보통 키는 초기에 설정된 값(예를 들어, 사용자가 입력한 값 또는 키 공유 알고리즘에서 생성된 값)에서 변경되지 않는바, 초기화 벡터만 변경하면 키 스트림은 새롭게 변경될 수 있다. 즉, 동일한 평문이 여러 번 전송된다 해도 초기화 벡터를 이용하여 항상 다른 암호문으로 암호화할 수 있다. 구체적으로, 시드는 키와 초기화 벡터를 순차적으로 연결하는 연접(concatenation)을 통하여 생성될 수 있다. 예를 들어, 사용자가 입력한 키는 40비트이고, 초기화 벡터는 24비트일 수 있으며, 이 경우 키와 초기화 벡터를 연접하여 64비트의 시드를 생성할 수 있다.

[0040] 본 발명의 일 실시예에서 초기화 벡터는 버스 시스템에 포함된 스트림 암호화 송수신부를 초기화시킬 수 있다. 예를 들어, 초기화 벡터를 0으로 할 경우 버스 시스템에 포함된 스트림 암호화 송수신부는 모두 초기화될 수 있다. 본 발명의 일 실시예에서 초기화 벡터의 사이즈는 N일 수 있고, 여기서 N은 32의 배수일 수 있다.

[0041] 명령어 식별자가 '0000' 및 '0001'이 아닌 그 외의 경우(others)는 바디에 포함된 데이터가 암호화되지 않은 것으로 간주하여, 이 경우 프레임에 포함된 바디 부분에 대한 복호화 동작을 수행할 필요가 없으므로 수신 모듈의 부하를 줄일 수 있다.

[0042] 도 6은 본 발명의 일 실시예에 따른 프레임의 종류를 나타내는 표이다.

[0043] 도 6을 참조하면, 프레임의 속성에 따라, 즉, 프레임의 바디에 데이터가 포함되어 있는지 또는 초기화 벡터가 포함되어 있는지에 따라 프레임의 종류는 데이터(data) 프레임 및 제어(control) 프레임의 두 가지로 분류할 수 있다.

[0044] 데이터 프레임은 헤더 및 바디로 구성되고, 바디에 암호화된 데이터가 포함된 것을 나타내고, 제어 프레임은 헤더 및 바디로 구성되고, 바디에 새로운 초기화 벡터가 암호화되어 포함된 것을 나타낸다.

[0045] 이하에서는 도 2 내지 도 6을 참조하여, 본 발명의 일 실시예에 따른 버스 시스템의 구체적인 동작을 설명하기로 한다.

[0046] 먼저, 제1 모듈(21)에서 제2 모듈(22)로 프레임이 전송되는 경우의 데이터의 암호화 및 복호화 방법을 설명하기로 한다. 여기서, 데이터는 제1 모듈(21)에서 제2 모듈(22)로 전송되는바, 제1 모듈(21)은 데이터의 송신 모듈이고, 제2 모듈(22)은 데이터의 수신 모듈로 설명하기로 한다. 그러나, 이는 일 실시예에 불과하고, 데이터가 제2 모듈(22)에서 제1 모듈(21)로 전송하는 것이 가능함은 물론이고, 이 경우 제2 모듈(22)은 데이터의 송신 모듈이고, 제1 모듈(21)은 데이터의 수신 모듈이 된다.

[0047] 제1 프레임 핸들러(211)는 전송할 프레임의 헤더에 프레임의 전송 순서를 나타내는 순서 번호(sequence number, SN) 및 바디에 포함된 데이터의 속성을 기록한다. 여기서, 바디에 포함된 데이터의 속성은 명령어 식별자로 기록될 수 있다. 제1 모듈(21)이 데이터를 전송하는 송신 모듈인 경우, 제1 프레임 핸들러(211)는 송신용 순서 번호(SNTx A)를 헤더에 기록한다. 또한, 제1 프레임 핸들러(211)는 전송할 프레임의 바디에 데이터 또는 초기화 벡터를 기록한다. 그리고, 제1 프레임 핸들러(211)는 새로운 초기화 벡터의 발생을 지시할 수 있고, 새로운 초기화 벡터가 발생된 경우 제1 스트림 암호화 송신부(212) 또는 제2 스트림 암호화 수신부(213)를 초기화할 수 있다.

[0048] 제1 시드 생성부(212)는 소정의 키(KEY)와 송신용 초기화 벡터(IV_T)를 연접함으로써 시드를 생성할 수 있다. 상술한 바와 같이, 키는 사용자가 입력한 값으로, 고정된 값일 수 있다. 그러나, 정기적 또는 부정기적으로 송신용 초기화 벡터(IV_T)를 변경하여 시드 값을 변경할 수 있다.

[0049] 제1 스트림 암호화 송신부(214)는 제1 시드 생성부(212)에서 출력된 시드로부터 키 스트림(KS)을 생성한다. 송신용 초기화 벡터(IV_T)가 갱신된 경우 제1 스트림 암호화 송신부(214)는 초기화된다. 본 발명의 다른 실시예에서, 제1 스트림 암호화 송신부(214)는 예비 스트림 암호화 송신부를 더 가질 수 있다. 송신용 초기화 벡터(IV_T)가 초기화될 때, 제1 스트림 암호화 송신부(214)의 서비스는 중단될 가능성이 있다. 그러나, 이 경우 예비 스트림 암호화 송신부가 제1 스트림 암호화 송신부(214)를 대신하여 암호화를 수행함으로써 서비스의 중단을 방지할 수 있으므로 시스템의 성능이 향상될 수 있다.

[0050] 제1 연산부(216)는 제1 프레임 핸들러(211)에서 출력된 프레임의 바디 부분과 생성된 키 스트림(KS)을 연산하여, 바디 부분에 포함된 데이터 또는 초기화 벡터를 암호화한다. 구체적으로, 제1 연산부(216)는 프레임의 바디 부분과 생성된 키 스트림(KS)에 대해 배타적 논리합(XOR)을 수행하여, 바디 부분에 포함된 데이터 또는 초기화 벡터를 암호화할 수 있다. 이 때, 제1 연산부(216)는 제1 프레임 핸들러(211)에서 출력된 프레임의 헤더 부분은 암호화하지 않는다. 따라서, 제1 프레임 핸들러(211)에서 출력된 프레임의 헤더는 암호화되지 않은 상태로 버스로 전송되고 프레임의 바디는 암호화된 상태로 버스로 전송되므로, 프레임의 헤더와 바디는 각각 버스로 전송된다.

[0051] 제2 프레임 핸들러(221)는 버스로부터 전송된 프레임의 헤더를 분석하여 헤더로부터 송신용 순서 번호(SNTx A)와 제2 프레임 핸들러(221)에 저장된 수신용 순서 번호(SNRx B)를 비교한다. 비교 결과, 송신용 순서 번호(SNTx A)가 수신용 순서 번호(SNRx B)와 일치하는 경우에 제2 프레임 핸들러(221)는 수신한 프레임의 바디 부분을 복호화하도록 제2 스트림 암호화 수신부(225)를 제어한다. 한편, 비교 결과, 송신용 순서 번호(SNTx A)가 수신용 순서 번호(SNRx B)와 일치하지 않는 경우에 수신한 프레임은 복호화하지 않고, 순서 번호를 초기화한다.

[0052] 다시 말해, 제2 프레임 핸들러(221)는 제2 모듈(22)에서 수신하고자 하는 데이터인 경우에만 수신한 프레임의 바디에 대한 복호화를 수행도록 제2 스트림 암호화 수신부(225)를 제어하고, 제2 모듈(22)에서 수신하고자 하는 데이터가 아닌 경우, 즉, 송신용 순서 번호(SNTx A)와 수신용 순서 번호(SNRx B)가 일치하지 않는 경우에는 수신한 프레임의 바디에 대한 복호화를 수행하지 않도록 제2 스트림 암호화 수신부(225)를 제어하고, 순서 번호를 초기화한다.

[0053] 제4 시드 생성부(223)는 소정의 키(KEY)와 수신용 초기화 벡터(IV_R)를 연접함으로써 시드를 생성할 수 있다. 상술한 바와 같이, 키는 사용자가 입력한 값으로, 고정된 값일 수 있다. 그러나, 정기적 또는 부정기적으로 수신용 초기화 벡터(IV_R)를 변경하여 시드 값을 변경할 수 있다.

[0054] 제2 스트림 암호화 수신부(225)는 제4 시드 생성부(223)에서 출력된 시드로부터 키 스트림(KS)을 생성한다. 수신용 초기화 벡터(IV_R)가 갱신된 경우 제2 스트림 암호화 수신부(225)는 초기화된다. 본 발명의 다른 실시예에서, 제2 스트림 암호화 수신부(225)는 예비 스트림 암호화 수신부를 더 가질 수 있다. 이 경우 수신용 초기화 벡터(IV_R)가 초기화될 때, 서비스의 중단을 방지할 수 있으므로 시스템의 성능이 향상될 수 있다.

[0055] 이 때, 송신용 초기화 벡터(IV_T)와 수신용 초기화 벡터(IV_R)는 동일하다. 그 결과, 제1 스트림 암호화 송신부(214)에서 생성되는 키 스트림(KS)과 제2 스트림 암호화 수신부(225)에서 생성되는 키 스트림(KS)은 동일하므로, 암호화된 데이터에 대한 정확한 복호화가 이루어질 수 있다.

[0056] 제2 연산부(226)는 제2 프레임 핸들러(221)에서 추출한 송신용 순서 번호(SNTx A)가 수신용 순서 번호(SNRx B)와 일치하는 경우 제2 프레임 핸들러(221)에서 출력된 프레임의 바디 부분과 생성된 키 스트림(KS)을 연산하여, 바디 부분에 포함된 데이터 또는 초기화 벡터를 복호화한다. 구체적으로, 제2 연산부(226)는 프레임의 바디 부분과 생성된 키 스트림(KS)에 대해 배타적 논리합(XOR)을 수행하여, 바디 부분에 포함된 데이터 또는 초기화 벡터를 복호화할 수 있다. 이 때, 제2 연산부(226)는 제2 프레임 핸들러(221)에서 출력된 프레임의 헤더 부분은 복호화하지 않는다.

[0057] 다음으로, 상술한 내용을 기초로 하여 초기화 벡터의 갱신 동작에 대하여 설명하기로 한다.

[0058] 초기화 벡터의 갱신은 데이터의 전송 과정에서 순서 번호가 불일치하는 경우 또는 미리 정해진 간격(interval)에 따라 이루어질 수 있다. 제1 및 제2 모듈(21, 22) 중 어느 모듈이든지 초기화 벡터를 갱신할 수 있다.

[0059] 제2 모듈(22)에 포함된 제2 프레임 핸들러(221)는 새로운 초기화 벡터(IV)를 바디에 포함시켜, 제어 프레임을 작성하여 버스를 통해 제1 모듈(21)에 포함된 제1 프레임 핸들러(211)에 제공한다. 또한, 제2 프레임 핸들러(221)는 새로운 초기화 벡터(IV)를 제3 시드 발생부(222)에 제공하여, 제3 시드 발생부(222)에서 이용되는 송신용 초기화 벡터(IV_T)를 갱신한다. 이로써, 제2 스트림 암호화 송신부(224)는 초기화되고, 새로운 키 스트림을 생성할 수 있다.

[0060] 제1 모듈(21)은 제어 프레임의 바디에 포함된 새로운 초기화 벡터(IV)를 복호화하고, 복호화된 초기화 벡터를 제2 시드 발생부(213)에 제공하여, 제2 시드 발생부(213)에서 이용되는 수신용 초기화 벡터(IV_R)를 갱신한다. 이로써, 제1 스트림 암호화 수신부(215)는 초기화되고, 새로운 키 스트림을 생성할 수 있다.

[0061] 그 결과, 제1 모듈(21)의 수신용 초기화 벡터(IVR)와 제2 모듈(22)의 송신용 초기화 벡터(IVT)는 일치하게 된다.

[0062] 도 7은 본 발명의 일 실시예에 따른 데이터 암호화 방법을 나타내는 흐름도이다.

[0063] 도 7을 참조하면, 본 실시예에 따른 데이터의 암호화 방법은 도 2에 도시된 버스 시스템에서 시계열적으로 처리되는 단계들로 구성된다. 따라서, 이하 생략된 내용이라 하더라도 도 2에 도시된 버스 시스템에 관하여 이상에서 기술된 내용은 본 실시예에 따른 데이터의 암호화 방법에도 적용된다.

[0064] 71 단계에서 데이터를 전송할 모듈은 프레임의 바디에 포함된 데이터와 키 스트림을 연산함으로써 암호화된 데이터를 버스로 전송한다. 여기서, 프레임은 헤더와 바디로 구성된 데이터의 전송 단위이며, 키 스트림은 소정의 키(key)와 초기화 벡터를 기초로 생성될 수 있다.

[0065] 72 단계에서 데이터를 전송할 모듈은 프레임의 전송 순서를 나타내는 순서 번호(sequence number)를 포함하는 헤더를 버스로 전송한다. 본 발명의 일 실시예에서, 헤더는 데이터의 속성 정보를 더 포함할 수 있으며, 데이터의 속성에 따라 프레임은 데이터 프레임 또는 제어 프레임으로 분류될 수 있다.

[0066] 이 때, 초기화 벡터가 갱신되는 경우 초기화 벡터를 프레임의 바디에 포함시키고, 키 스트림과 초기화 벡터를 연산하여 초기화 벡터를 암호화할 수도 있다.

[0067] 도 8은 본 발명의 일 실시예에 따른 데이터 복호화 방법을 나타내는 흐름도이다.

[0068] 도 8을 참조하면, 본 실시예에 따른 데이터의 복호화 방법은 도 2에 도시된 버스 시스템에서 시계열적으로 처리되는 단계들로 구성된다. 따라서, 이하 생략된 내용이라 하더라도 도 2에 도시된 버스 시스템에 관하여 이상에서 기술된 내용은 본 실시예에 따른 데이터의 복호화 방법에도 적용된다.

[0069] 81 단계에서 데이터를 수신하는 모듈은 수신용 순서 번화를 버스로 전송된 프레임의 헤더로부터 추출한 발신용 순서 번호와 비교한다. 비교 결과, 수신용 순서 번호와 발신용 순서 번호가 일치하는 경우에는 82 단계를 수행하고, 일치하지 않는 경우에는 프레임의 바디 부분을 복호화하지 않고 초기화 벡터의 갱신을 요청할 수 있다.

[0070] 82 단계에서 데이터를 수신하는 모듈은 버스로 전송된 프레임의 바디에 포함된 데이터와 키 스트림을 연산하여 데이터를 복호화한다. 이 때, 키 스트림은 소정의 키와 초기화 벡터를 기초로 생성될 수 있다.

[0071] 도 9은 본 발명의 일 실시예에 따른 데이터 암호화 및 복호화 방법이 적용될 수 있는 예를 나타내는 개략도이다.

[0072] 도 9를 참조하면, 본 발명의 일 실시예에 따른 데이터 암호화 및 복호화 방법은 PCI(peripheral component interconnect, 92)와 같은 오픈 버스를 통하여 데이터를 전송하는 호스트(91)와 개발 보드(93) 사이에 적용될 수 있다. 여기서, PCI는 중앙처리장치(CPU)와 주변 장치를 연결하는 로컬 버스를 의미하며, 오픈 버스는 외부 기기에 자유롭게 접속할 수 있는 버스를 의미한다.

[0073] 본 발명의 일 실시예에 따른 데이터 암호화 및 복호화 방법은 기존의 버스 시스템에 대하여 하드웨어의 수정을 필요하지 않다. 도 9에서 호스트와 개발 보드로 나타낸 것은 하드웨어로 한정하지 않고, 소프트웨어와 하드웨어, 하드웨어와 하드웨어 및 소프트웨어와 소프트웨어 사이의 데이터의 전송에 모두 적용가능하기 때문이다.

[0074] 본 발명은 상술한 실시예에 한정되지 않으며, 본 발명의 사상 내에서 당업자에 의한 변형이 가능함은 물론이다.

[0075] 본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 하드디스크, 플로피디스크, 플래쉬 메모리, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드로서 저장되고 실행될 수 있다.

발명의 효과

[0076] 본 발명에 따르면, 소정의 키(key)와 초기화 벡터를 기초로 생성된 키 스트림과 프레임의 바디에 포함된 데이터를 연산하여 암호화된 데이터를 버스로 전송하고, 프레임의 전송 순서를 나타내는 순서 번호(sequence number) 및 데이터의 속성을 나타내는 프레임의 헤더를 버스로 전송함으로써, 송수신 모듈의 순서 번호가 일치하는 경우에만 복호화를 수행할 수 있으며, 그 결과 버스 상에서 전송되는 데이터에 대한 보안성이 향상될 수 있다. 즉, 버스를 태핑하여도 암호화된 데이터를 판독하기 어렵다.

[0077] 또한, 본 발명에 따르면, 종래의 버스 시스템에서 하드웨어의 수정이 필요하지 않아서 새로운 모듈로의 확장이 용이하며, 소프트웨어 및/또는 하드웨어 사이의 다양한 환경에 적용할 수 있다.

도면의 간단한 설명

[0001] 도 1은 종래의 스트림 암호 시스템을 나타내는 블록도이다.

[0002] 도 2는 본 발명의 일 실시예에 따른 버스 시스템을 나타내는 블록도이다.

[0003] 도 3은 본 발명의 일 실시예에 따른 프레임의 구조를 나타내는 개략도이다.

[0004] 도 4는 도 3의 프레임에 포함된 헤더의 구조를 나타내는 개략도이다.

[0005] 도 5는 도 4의 헤더에 포함된 명령어 식별자를 나타내는 표이다.

[0006] 도 6은 본 발명의 일 실시예에 따른 프레임의 종류를 나타내는 표이다.

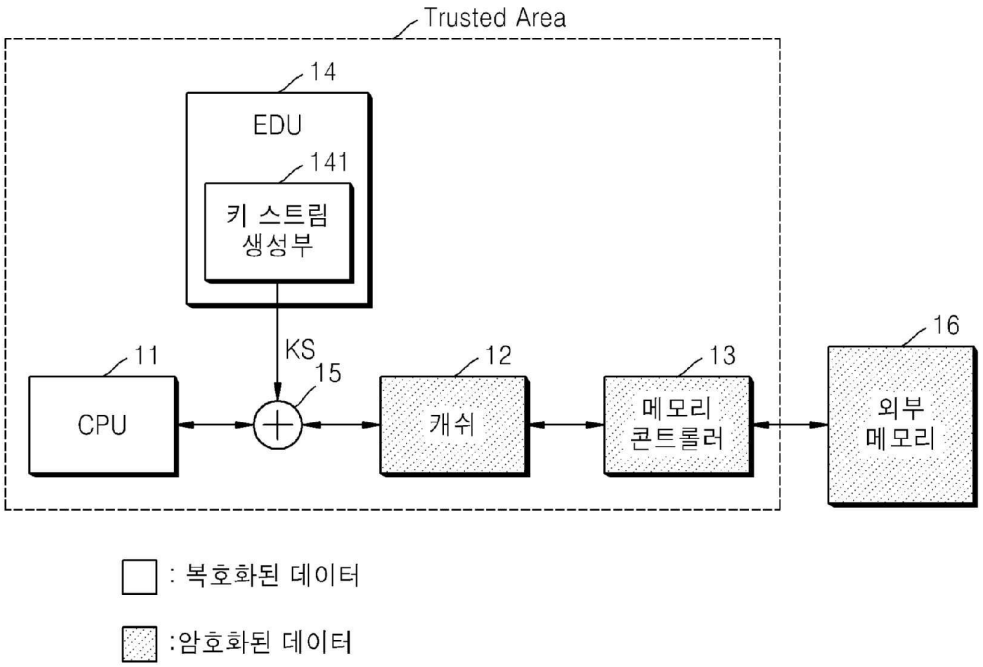
[0007] 도 7은 본 발명의 일 실시예에 따른 데이터 암호화 방법을 나타내는 흐름도이다.

[0008] 도 8은 본 발명의 일 실시예에 따른 데이터 복호화 방법을 나타내는 흐름도이다.

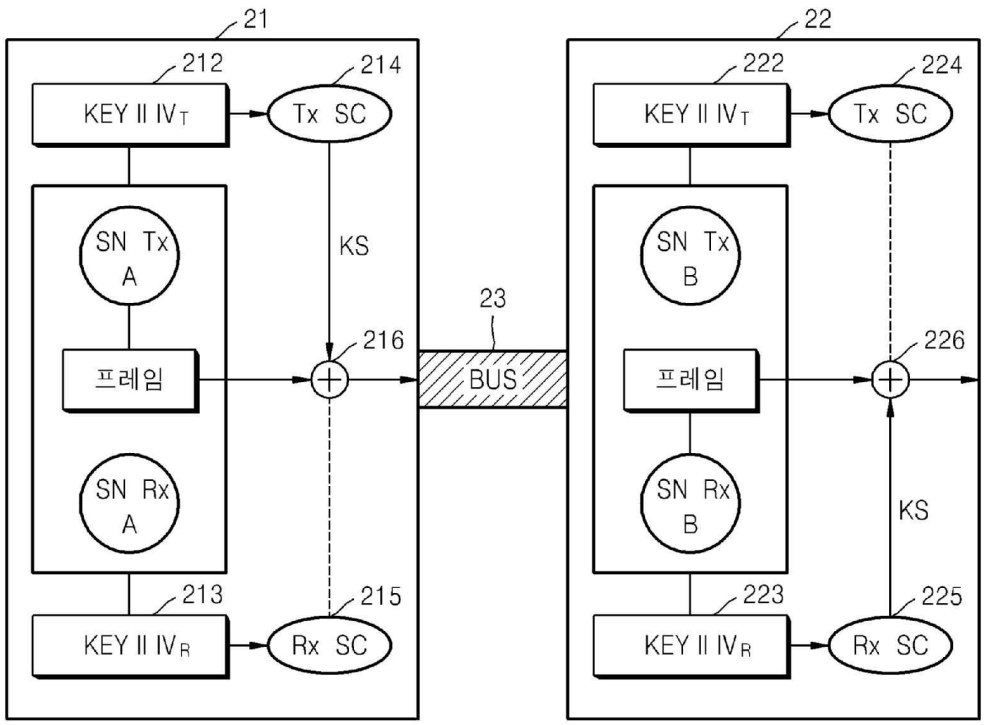
[0009] 도 9은 본 발명의 일 실시예에 따른 데이터 암호화 및 복호화 방법이 적용될 수 있는 예를 나타내는 개략도이다.

도면

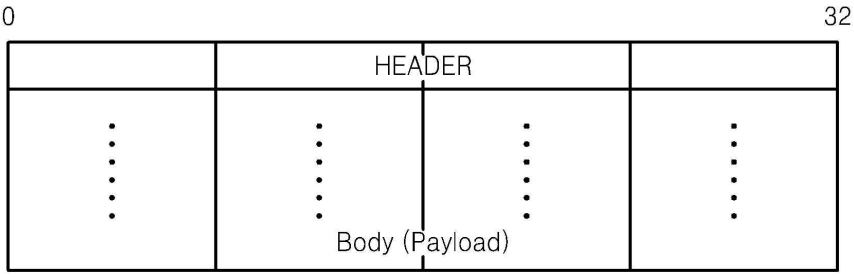
도면1



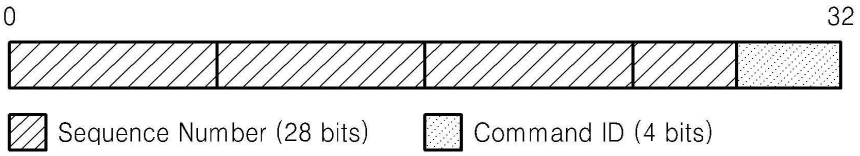
도면2



도면3



도면4



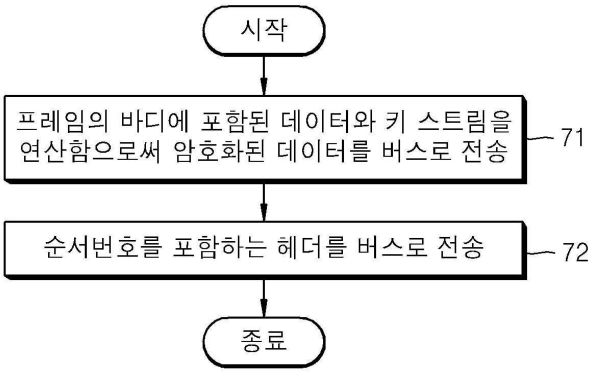
도면5

Command ID	Description
0000	Data Payload (Body) Encrypted.
0001	New Init Vector Included in the payload (IV has size N, where N is a multiple of 32).
Others	Reserved.

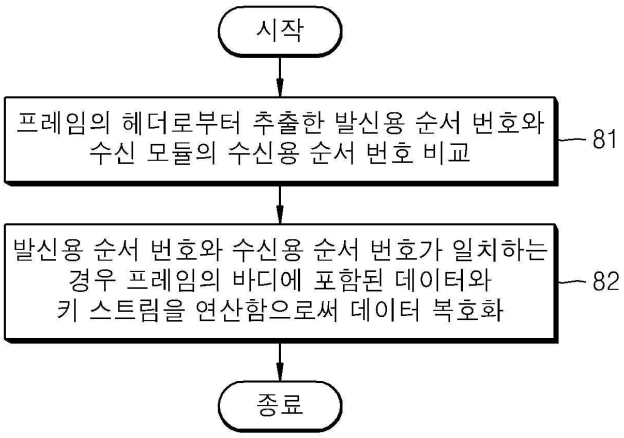
도면6

Frame Type	Description
Data	Header+Body (Payload)로 구성, Payload는 Encrypt된 Data가 위치.
Control	Header+Body (Payload)로 구성, Payload는 새로운 IV값이 Encrypt되어 들어 있음.

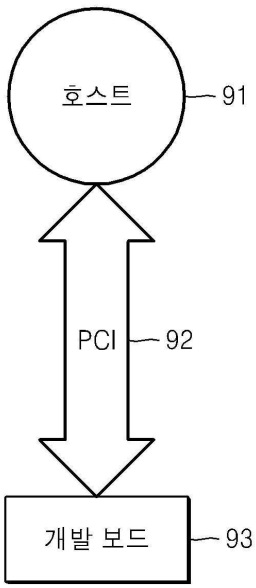
도면7


시작
프레임의 바디에 포함된 데이터와 키 스트림을 연산함으로써 암호화된 데이터를 버스로 전송
71
순서번호를 포함하는 헤더를 버스로 전송
72
종료

도면8


시작
프레임의 헤더로부터 추출한 발신용 순서 번호와 수신 모듈의 수신용 순서 번호 비교
81
발신용 순서 번호와 수신용 순서 번호가 일치하는 경우 프레임의 바디에 포함된 데이터와 키 스트림을 연산함으로써 데이터 복호화
82
종료

도면9


호스트
91
PCI
92
개발 보드
93