(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[8]
H04L 9/06 (2006.01)
H04L 9/28 (2006.01)

(11) 공개번호 10-2006-0011999
(43) 공개일자 2006년02월06일

(21) 출원번호 10-2005-7021575
(22) 출원일자 2005년11월11일
번역문 제출일자 2005년11월11일
(86) 국제출원번호 PCT/ES2004/000206
국제출원일자 2004년05월11일
(87) 국제공개번호 WO 2004/102869
국제공개일자 2004년11월25일

(30) 우선권주장 P 2003 01104 2003년05월13일 스페인(ES)

(71) 출원인 디세노 데 시스테마스 엔 실리시오, 에스.에이.
스페인 46980 파테르나(발렌시아) 2/파끄 테크놀로지코 샬레스 로버트 다윈

(72) 발명자 블라스코 클라레 호르제 비센테
스페인 이-46020 발렌시아 23-2-38 구아르디아 시빌
리베이로 인수아 후안 카를로스
스페인 이-46019 발렌시아 푸에르타43 30-이에스씨. 비-10°베아타 겐
노베바 토레스
에스테베 로레 마리아
스페인 이-46009 발렌시아 5 - 푸에르타 11 길 로게르

(74) 대리인 하상구
하영욱

심사청구 : 없음

(54) D E S 알고리즘에 의거한 암호화 기법

요약

본 발명은 DES 알고리즘에 의거한 암호화 기법에 관한 것이다. 본 발명은 네트워크에 접속된 사용자 장치 또는 노드 사이에서 데이터 패킷을 송신하는 통신 시스템에 사용될 수 있다. 본 발명에 의한 기법은 DES 암호 알고리즘을 사용하여 각 패킷을 암호화하는데 사용되는 각 패킷마다 다른 랜덤 키(6)를 생성하는 단계, 및 DES 알고리즘보다 더 안전한 알고리즘을 사용하여 암호화된(9), 패킷의 헤딩내의 랜덤 키(6)를 송신하는 단계로 이루어지는 것을 특징으로 한다. 이러한 방식으로, 본 발명은 DES 암호 알고리즘을 대신해 향상된 기법을 사용하여, 통신 시스템의 노드 및 사용자 장치가 접속된 안전하지 않은 매체를 통한 전송에 관련해서 보안성을 향상시키는데 사용될 수 있다

대표도

도 1

색인어

암호화 기법, DES 알고리즘

명세서

기술분야

상기 발명의 명칭에 표현된 바와 같이, 본 발명은 하드웨어가 네트워크에 접속된 사용자 또는 노드간에 전송된 데이터 패킷을 암호화 할 수 있도록 한 종래의 DES(Data Encryption Standard) 알고리즘에 의거한 암호화 절차에 관한 것이다.

본 발명은 DES 암호화 알고리즘을 대신하여 본 발명의 절차를 이용하여 전기 통신 시스템의 노드 또는 장치 사이에 안전하지 않은 매체상의 전송의 보안성을 향상시키는 새로운 완전 랜덤 키(key)로 각 데이터 패킷을 암호화 하고 시스템의 보안성을 향상시키는 키의 랜덤 생성을 특징으로 한다.

배경기술

대부분의 전기 통신 시스템에 있어서, 외부인에 의한 데이터의 방수(傍受) 및/또는 변경에 대한 방지를 위해 정보상에 암호화 처리가 수행될 필요가 있다.

DES는 암호 알고리즘의 표준으로서 1977년부터 미국 정부에 의해 사용되고 있다.

DES는 하드웨어와 소프트웨어 모두에서 실시가 매우 용이한 치환, 및 대치 연산이 이용되는 56비트 키에 의해 암호화되는 데이터 패킷 또는 64비트 블럭의 암호 알고리즘이다. 또한, 동일한 키가 데이터의 암호화 및 해독화 모두에 순차적으로 사용되기 때문에 DES는 대칭 알고리즘이다.

그것을 목적으로 공개된 FIBS(the First Internet Backgammon Server) PUB 46 문서에서 볼 수 있는 바와 같이, 이 알고리즘은 공지된 것이고, 암호 기법에 관한 여러가지 논문과 조약에 있어서 널리 기술되고 있으며, 1977년 1월 15일에 미국 국립 표준국(National Bureau of Standards)에 의해 국제 표준으로 승인되었다.

또한, 그 분야의 공지기술은 TDES(Triple DES) 또는 AES(Advanced Encryption Standard) 알고리즘과 같은 데이터의 방지, 및 보안 능력이 우수한 다른 암호 알고리즘이다. TDES 암호 알고리즘은 세개의 다른 키로 DES 알고리즘을 이용하여 세 번 연속으로 정보를 암호화 하는 것으로 이루어지는 DES 알고리즘의 변형이다. 한편, AES 알고리즘은 128, 192, 및 최대 256 비트의 키를 사용하며 DES 알고리즘보다 우수한 보안성과 속도의 조합을 제공한다.

이 중 어느 하나의 알고리즘으로 암호화된 메시지를 해독화하기 위해, 키의 철저한 테스트가 수행되어야 한다. 이것은 표준 DES에 있어서 2^{56} 이 필요한 것으로 계산되는 반면, TDES 버젼에 있어서 이 수치는 2^{112} 의 시도가 된다.

본 발명에 의한 절차의 장점은 이것을 사용하는 통신 시스템에 있어서, DES와 유사한 수준의 저감된 복잡성으로, 보호 능력이 우수한 알고리즘(TDES 또는 AES 등)과 대등한 보안성이 달성된다는 것이다. 이것을 달성하기 위해, 키의 생성은 완전히 랜덤 방식으로 이루어져 각 전송 데이터 패킷과 각 사용자마다 키가 달라지지 않으면 안된다. 이것에 의해, 그리고, 본 발명의 절차에 의해, 승인되지 않은 방수가 메시지를 해독할 수 없도록 하기 위해 송신된 각 패킷에 대한 시행착오의 전체 처리를 반복할 필요가 있고, 이렇게 얻어진 어느 정보도 후속 패킷을 해독할 목적으로서 사용될 수 없음으로 안전하고 효과적인 방식으로 시스템을 보호한다.

발명의 상세한 설명

이러한 목적을 달성하고 상기한 결점을 극복하기 위해, 본 발명은 데이터 패킷이 네트워크에 접속된 장치간에 전송되는 통신 시스템에 적용할 수 있는 DES 알고리즘에 의거한 암호화 절차로 이루어진다. 송신시, 이 절차는 DES 알고리즘에 의해 암호화될 각 데이터 패킷을 위해 백색 또는 유색 잡음에 의해 오염된 실제 신호에 의거하여 랜덤 키가 생성되는 것을 특징으로 한다. 이 패킷은 패킷용으로 생성된 랜덤 키와 DES 알고리즘에 의해 암호화 된다. 또한, 랜덤 키는 DES에 비해 보호 및 보안 능력이 우수한 암호 알고리즘에 의해 순차적으로 암호화 되고, 즉 결과적으로, 암호화된 키는 송신될 데이터 패킷의 헤더로 도입된다.

수신시, 절차는 수신된 패킷의 헤더로부터 암호화된 키가 추출되며, 상기 암호화된 키는 송신에 사용되는 DES에 비해 보호 및 보안 능력이 우수한 동일한 암호 알고리즘에 의해 해독되는 것을 특징으로 한다. 이러한 방식에 의해, 송신시의 패킷용으로 얻어진 랜덤 키가 다시 얻어진다. 이어서, 수신된 패킷은 얻어진 랜덤 키에 의해 해독되어, 송신되었어야 할 원본 정보가 다시 얻어진다.

또한, DES에 비해 보호 및 보안 능력이 우수한 암호 알고리즘은 각 사용자에 대해 하나 이상의 다른 암호화 키를 순차적으로 사용하고, 이 키는 송신 및 수신시에 각 사용자마다 랜덤하고 상이하다.

절차를 물리적으로 실시할 수 있게 하기 위해, 랜덤 키를 암호화하고 데이터 패킷의 암호화된 키를 생성하는데 필요한 키는 송신기 및 수신기에게 알려지고 수많은 사용자 장치의 기능으로서 가변 용량 메모리에 기억되도록 되어야 한다. 또한, 동일한 방식으로, 수신시에 암호화된 키를 해독하는데 필요한 키는 송신시 및 수신시에 알려지고 수많은 사용자 장치의 기능으로서 가변 용량 메모리에 기억된다.

이러한 방식으로, 통신 시스템에 있어서 암호화하는 이 방법과 유사한 수준의 복잡성에 의해 DES 알고리즘을 대신하여 이 절차를 사용하는 시스템의 보안성을 향상시키는데 성공하였다.

도면의 간단한 설명

도 1은 암호화된 데이터 패킷의 송신에 관한 본 발명에 의한 절차 실시를 위한 가능한 실시형태의 블럭도를 개략적으로 나타낸다.

도 2는 암호화된 데이터 패킷의 수신에 관한 본 발명에 의한 절차 실시를 위한 가능한 실시형태의 블럭도를 개략적으로 나타낸다.

도 3은 랜덤 키 생성에 관한 본 발명에 의한 절차의 실시형태에 사용될 수 있는 시프트 레지스터로 구성된 랜덤 키 생성기와 랜덤 입력 신호를 나타낸다.

실시예

첨부도면에 적용된 부호를 참조하여 본 발명의 예를 이하 상세히 설명한다.

본 발명에 관한 상기 설명에 언급된 바와 같이, 본 발명이 의도하는 목적은 TDES 또는 AES 등의 더 복잡한 암호화 시스템에 필적할 수 있도록 DES 알고리즘의 보안 레벨을 향상시킨 반면에 DES 알고리즘과 유사한 수준의 복잡성을 갖도록하는 보안성을 갖는 암호화 기법을 제공하는 것이다.

본 실시형태에 있어서, TDES 알고리즘은 DES로 데이터 패킷을 암호화하는 처리에 사용되는 키를 암호화하는데 사용된다. 상기 TDES 알고리즘은 암호화를 수행하는데 세개의 키를 필요로한다.

이것을 달성하기 위해, 본 발명의 절차를 사용한 통신 시스템은 키의 랜덤 생성기(5)(도 1 참조)를 사용하며, 이 랜덤 생성기(5)는 도 3에 도시된 바와 같이 배열되며, DES 알고리즘에서 64 비트인 키를 생성하는데 필요한 비트의 폭을 갖는 시프트 레지스터(25)로 구성된다. 시프트 레지스터로의 입력(24)은 일반적으로 실제 통신 채널을 통해 송신된 신호를 오염시키는 백색 또는 유색 잡음에 의해 오염된 신호(22)의 비트로 이루어진다. 잡음에 의해 오염되기 때문에, 이 신호(22)는 그 수치가 예컨대, 아날로그-디지털 컨버터(23)를 사용하여 2진수로 양이 계측되면 완전 랜덤한 최저 비트를 갖는다. 이는, 각 클럭 싸이클에서 입력으로서 이 비트 중 하나를 취하고 레지스터의 내용을 시프트하면, 시프트 레지스터의 폭과 동일한 싸이클의 수를 따르는 레지스터의 모든 비트가 랜덤하게 되고 그 레지스터의 수치는 이하 설명되어질 송신될 실제 데이터 패킷의 암호화를 위한 랜덤 키(6)로서 사용될 수 있는 방식으로 수행된다. 이러한 키 생성의 처리는 송신되는 각 데이터 패킷의 반복되는데, 모든 키(6)는 완전히 랜덤하게 생성되고 서로 독립적이다.

도 1은 통신 시스템 내의 송신에 있어서 본 발명의 절차를 실시하는 소자에 있어서의 일반적 기능의 예에 대한 블럭도를 나타낸다.

송신시에 있어서, 인커밍 데이터 패킷(1)은 사용자(3)가 전송되는 대응 정보를 헤더로부터 얻기 위해 컨트롤 모듈(2)에서 분석된다. 수신이 알려지면, 수신에 대응하는 세개의 키(7)는 메모리(4)로부터 추출된다.

이 세개의 키(7)는 본 발명이 랜덤 생성기(5)에 의해 생성된 랜덤 키(6)의 암호화에 사용하는 TDES 알고리즘(8)의 애플리케이션을 위해 사용될 것이다. 또한, 이 세개의 키도 순차적으로 각 사용자마다 랜덤한 방식으로 생성된다. 이러한 방식으로, 암호화된 키(9)가 얻어진다.

랜덤 키(6)에 의해 암호화 이전에 패킷의 데이터는 전송을 위해 현재 암호화된 데이터 패킷(11)을 얻는 DES 알고리즘에 의해 모듈(10)내에서 암호화된다. 수신시의 패킷을 디코딩하기 위해, 랜덤 키(6)를 전송할 필요가 있지만, 데이터의 암호화 후 모듈(10)은 패킷(11)의 헤더로 암호화된 키(9)를 도입한다. 이러한 방식으로, 수신시의 패킷을 해독할 수 있게 하기 위해 암호화된 키를 해독할 필요가 있다.

도 2는 통신 시스템내의 수신에 있어서의 본 발명의 절차를 실시하는 소자의 일반적인 기능의 예에 대한 블럭도를 나타낸다.

수신시에 있어서, DES 및 TDES 알고리즘의 대칭성에 의해 처리는 반대가 되지만 송신시에 있어서 방식은 상기 하나의 것과 유사하게 사용될 수 있다.

이러한 경우에 있어서, 컨트롤 모듈(13)은 패킷이 송신되는 사용자(14)의 정보와 암호화된 키(9)를 인커밍 데이터 패킷(12)으로부터 얻는다. 이 암호화된 키(9)는 패킷마다 랜덤한 키(6)이지만, 수신하는 사용자가 아는 세개의 키(7)로 송신시에 있어서 TDES에 의해 암호화된다.

암호화된 키(9)는 TDES 알고리즘과 세개의 키(7)에 의해 모듈(18)에서 해독된다. 세개의 키는 송신기 사용자(14)의 정보가 인덱싱된 메모리(15)로부터 추출된다. 암호화된 키(9)가 해독되는 경우, 전송시에 있어서 데이터의 암호화에 사용되는 키(6)가 얻어진다.

일단 키(6)가 해독되면, 데이터는 DES 알고리즘에 의해 모듈(20)내에서 해독되고, 원래 데이터(1)가 성공적으로 얻어진다.

(57) 청구의 범위

청구항 1.

데이터 패킷이 네트워크에 접속된 장치간에 전송되는 통신 시스템에 적용할 수 있는 DES 알고리즘에 의거한 암호화 기법으로서:

송신시에,

상기 DES 알고리즘에 의해 암호화될 상기 각 데이터 패킷을 위해 백색 및 유색 잡음 사이로부터 선택된 잡음에 의해 오염된 실제 신호에 의거하여 랜덤 키(6)를 생성하는 단계;

데이터 패킷용으로 생성된 상기 랜덤 키와 상기 DES 알고리즘에 의해 상기 데이터 패킷을 암호화하는 단계;

상기 DES에 비해 보호 및 보안 능력이 우수한 암호 알고리즘에 의해 상기 랜덤 키(6)를 암호화하는 단계; 및

송신될 상기 데이터 패킷의 헤더로 상기 암호화된 키(9)를 도입하는 단계를 포함하는 것을 특징으로 하는 DES 알고리즘에 의거한 암호화 기법.

청구항 2.

제 1 항에 있어서,

수신시에,

수신된 패킷의 헤더로부터 상기 암호화된 랜덤 키(9)를 추출하는 단계;

상기 랜덤 키(6)를 얻기 위해 전송시에 사용되는 DES(18)에 비해 보호 및 보안 능력이 우수하고 동일한 암호 알고리즘에 의해 상기 암호화된 랜덤 키(9)를 해독하는 단계; 및

상기 얻어진 랜덤 키(6)에 의해 상기 수신된 패킷을 해독화하는 단계를 포함하는 것을 특징으로 하는 DES 알고리즘에 의거한 암호화 기법.

청구항 3.

제 1 항 또는 제 2 항에 있어서,

DES에 비해 보호 및 보안 능력이 우수한 상기 암호 알고리즘은 각 사용자에 대해 하나 이상의 다른 암호화 키(7)를 순차적으로 사용하는 것을 특징으로 하는 DES 알고리즘에 의거한 암호화 기법.

청구항 4.

제 3 항에 있어서,

상기 데이터 키에 더 안전한 암호 알고리즘을 적용하기 위해 필요한 상기 하나 이상의 암호화 키(7)는 송신시 및 수신시에 각 사용자마다 랜덤하고 다르다는 것을 특징으로 하는 DES 알고리즘에 의거한 암호화 기법.

청구항 5.

제 1 항에 있어서,

상기 랜덤 키(6)를 암호화하고, 상기 데이터 패킷의 암호화된 키(9)를 생성하는데 필요한 상기 하나 이상의 키(7)는 송신기 및 수신기에 알려지고, 송신시에 수많은 사용자 장치의 기능으로서 가변 용량 메모리(4)내에 기억되는 것을 특징으로 하는 DES 알고리즘에 의거한 암호화 기법.

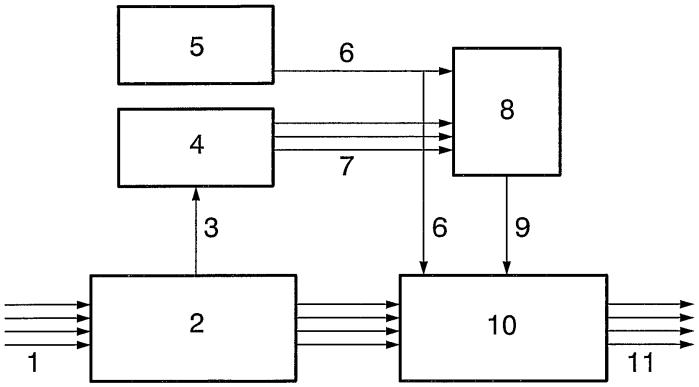
청구항 6.

제 2 항 또는 제 3 항에 있어서,

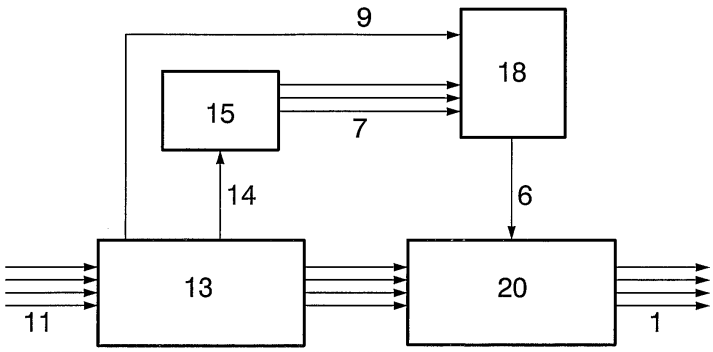
상기 랜덤 키(9)를 해독하고 상기 데이터 패킷의 해독된 키(6)를 생성하는데 필요한 상기 하나 이상의 키(7)는 송신기 및 수신기에 알려지고, 수신시에 상기 수많은 사용자 장치의 기능으로서 가변 용량 메모리(15)내에 기억되는 것을 특징으로 하는 DES 알고리즘에 의거한 암호화 기법.

도면

도면1



도면2



도면3