(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0055337
(43) 공개일자 2009년06월02일

(51) Int. Cl.
H04L 9/28 (2006.01) *H04L 12/22* (2006.01)
(21) 출원번호 10-2007-0122208
(22) 출원일자 2007년11월28일
심사청구일자 2007년11월28일

(71) 출원인
울산대학교 산학협력단
울산 남구 무거2동 산29
(72) 발명자
공형윤
울산광역시 중구 약사동 707-48 래미안 2차 203-1105
(74) 대리인
장한특허법인

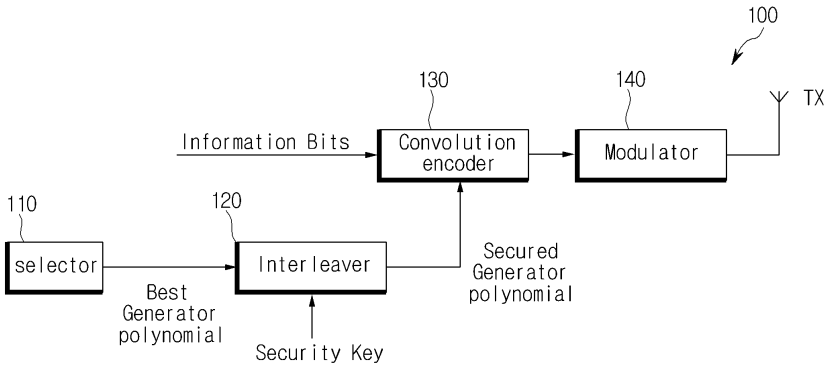
전체 청구항 수 : 총 8 항

(54) 물리계층에서 콘볼루션 부호를 이용한 무선 센서 네트워크보안 시스템 및 방법

(57) 요 약

본 발명에 따르면, 시스템이 요구하는 특정한 콘볼루션 부호 그룹을 선택받고, 상기 특정한 콘벌루션 부호 그룹 내의 콘볼루션 부호 생성 다항식 중, 특정 자유거리를 갖는 어느 일 콘볼루션 부호 생성 다항식을 선택받는 선택부; 상기 선택부에서 선택받은 콘볼루션 부호 생성 다항식을 보안키를 이용하여 랜덤하게 인터리빙하는 인터리버; 및 전송하고자 하는 정보비트를 상기 인터리버에서 인터리빙된 콘볼루션 부호 생성 다항식을 이용하여 인코딩하는 콘볼루션 인코더;를 포함하는 물리계층에서 콘볼루션 부호를 이용한 무선 센서 네트워크 보안 시스템 및 그 방법이 제공된다. 개시된 무선 센서 네트워크 보안 시스템 및 방법에 따르면, 무선 센서 네트워크(WSN) 환경에서 정보 교환시 채널 부호화 기법인 콘볼루션 부호화 기법과 보안키를 이용하여 데이터의 비화성능을 향상시키고 물리계층에서부터 정보를 보호함과 동시에 에러정정이 가능하도록 하는 이점이 있다.

대 표 도 - 도1



특허청구의 범위

청구항 1

시스템이 요구하는 특정한 콘볼루션 부호 그룹을 선택받고, 상기 특정한 콘벌루션 부호 그룹 내의 콘볼루션 부호 생성 다항식 중, 특정 자유거리를 갖는 어느 일 콘볼루션 부호 생성 다항식을 선택받는 선택부;

상기 선택부에서 선택받은 콘볼루션 부호 생성 다항식을 보안키를 이용하여 랜덤하게 인터리빙하는 인터리버; 및

전송하고자 하는 정보비트를 상기 인터리버에서 인터리빙된 콘볼루션 부호 생성 다항식을 이용하여 인코딩하는 콘볼루션 인코더를 포함하는 물리계층에서 콘볼루션 부호를 이용한 무선 센서 네트워크 보안 시스템.

청구항 2

제 1항에 있어서, 상기 선택부는,

상기 특정한 콘벌루션 부호 그룹 내의 콘볼루션 부호 생성 다항식 중 자유거리가 가장 큰 상계(上界)의 콘볼루션 부호 생성 다항식을 선택받고,

상기 인터리버는,

상기 선택부에서 선택받은 콘볼루션 부호 생성 다항식을 이진 형태로 배열한 행렬에 관한 행을 보안키를 이용하여 랜덤하게 인터리빙하는 것을 특징으로 하는 물리계층에서 콘볼루션 부호를 이용한 무선 센서 네트워크 보안 시스템.

청구항 3

제 1항에 있어서, 상기 선택부는,

상기 특정한 콘벌루션 부호 그룹 내의 콘볼루션 부호 생성 다항식 중 자유거리가 가장 큰 경우인 상계(上界)에 근접한 자유거리를 갖는 어느 일 콘볼루션 부호 생성 다항식을 선택받고,

상기 인터리버는,

상기 선택부에서 선택받은 콘볼루션 부호 생성 다항식을 이진 형태로 배열한 행렬에 관한 행과 열을 보안키를 이용하여 랜덤하게 인터리빙하는 물리계층에서 콘볼루션 부호를 이용한 무선 센서 네트워크 보안 시스템.

청구항 4

제 1항 내지 제 3항 중 어느 한 항에 있어서, 상기 보안키는,

정보비트를 전송하는 소스 측의 정보 및 상기 콘볼루션 인코더에 의해 인코딩된 정보비트를 전송받는 목적지 측의 정보를 각각 조합한 것을 특징으로 하는 물리계층에서 콘볼루션 부호를 이용한 무선 센서 네트워크 보안 시스템.

청구항 5

시스템이 요구하는 특정한 콘볼루션 부호 그룹을 선택받는 콘볼루션 부호 그룹 선택 단계;

상기 콘볼루션 부호 그룹 단계에서 선택된 특정한 콘벌루션 부호 그룹 내의 콘볼루션 부호 생성 다항식 중, 특정 자유거리를 갖는 어느 일 콘볼루션 부호 생성 다항식을 선택받는 생성 다항식 선택 단계;

상기 생성 다항식 선택 단계에서 선택받은 콘볼루션 부호 생성 다항식을 보안키를 이용하여 랜덤하게 인터리빙하는 인터리빙 단계; 및

전송하고자 하는 정보비트를 상기 인터리빙된 콘볼루션 부호 생성 다항식을 이용하여 인코딩하는 콘볼루션 인코딩 단계를 포함하는 물리계층에서 콘볼루션 부호를 이용한 무선 센서 네트워크 보안 방법.

청구항 6

제 1항에 있어서, 상기 생성 다항식 선택 단계는,

상기 특정한 콘벌루션 부호 그룹 내의 콘볼루션 부호 생성 다항식 중 자유거리가 가장 큰 상계(上界)의 콘볼루션 부호 생성 다항식을 선택받고,

상기 인터리빙 단계는,

선택받은 콘볼루션 부호 생성 다항식을 이진 형태로 배열한 행렬에 관한 행을 보안키를 이용하여 랜덤하게 인터리빙하는 것을 특징으로 하는 물리계층에서 콘볼루션 부호를 이용한 무선 센서 네트워크 보안 방법.

청구항 7

제 1항에 있어서, 상기 생성 다항식 선택 단계는,

상기 특정한 콘벌루션 부호 그룹 내의 콘볼루션 부호 생성 다항식 중 자유거리가 가장 큰 경우인 상계(上界)에 근접한 자유거리를 갖는 어느 일 콘볼루션 부호 생성 다항식을 선택받고,

상기 인터리빙 단계는,

선택받은 콘볼루션 부호 생성 다항식을 이진 형태로 배열한 행렬에 관한 행과 열을 보안키를 이용하여 랜덤하게 인터리빙하는 물리계층에서 콘볼루션 부호를 이용한 무선 센서 네트워크 보안 방법.

청구항 8

제 5항 내지 제 7항 중 어느 한 항에 있어서, 상기 보안키는,

정보비트를 전송하는 소스 측의 정보 및 상기 콘볼루션 인코더에 의해 인코딩된 정보비트를 전송받는 목적지 측의 정보를 각각 조합한 것을 특징으로 하는 물리계층에서 콘볼루션 부호를 이용한 무선 센서 네트워크 보안 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 물리계층에서 콘볼루션 부호를 이용한 무선 센서 네트워크 보안 시스템 및 방법에 관한 것으로서, 보다 상세하게는 무선 센서 네트워크를 통한 정보 교환시 콘볼루션 부호화 기법과 보안키를 이용하여 데이터의 비화성능을 향상시킬 수 있는 물리계층에서 콘볼루션 부호를 이용한 무선 센서 네트워크 보안 시스템 및 방법에 관한 것이다.

배 경 기 술

<2> 일반적으로 무선 센서 네트워크(WSN;Wireless Sensor Network)를 위한 데이터 전송채널은 불특정 다수의 사용자에게 노출되어 있어 중요한 정보가 누출될 가능성이 상존하고 있다.

<3> 이러한 문제점을 해결하기 위하여 현재는 네트워크 계층에서 프로그램적으로 암호화를 수행하거나 PN(Pseudo Noise)코드를 이용하여 CDMA(Code Division Multiple Access) 방식으로 정보를 전송하게끔 하여 보안성을 강화하고 있다.

<4> 그러나, 정보의 원천적인 보안을 위해서는 물리계층에서 암호화가 필요하다.

<5> 또한, 무선 네트워크를 통해 전송되는 데이터는 무선 채널을 통과할 때 열잡음(AWGN;Additive White Gaussian Noise), 페이딩(Fading) 등과 같은 다양한 형태의 각종 잡음이 혼입되면서 많은 데이터 오류를 유발하게 된다. 이러한 데이터 오류를 정정하여 정확한 데이터를 복원하기 위하여 고려되어야 할 사항으로 수신데이터에 대한 에러정정 기능이 필요하게 된다.

발명의 내용

해결 하고자하는 과제

<6> 본 발명은 상술한 문제점을 해결하기 위하여 창출된 것으로서, 무선 센서 네트워크(WSN) 환경에서 정보 교환시 채널 부호화 기법인 콘볼루션 부호화 기법과 보안키를 이용하여 데이터의 비화성능을 향상시키고 물리계층에서

부터 정보를 보호함과 동시에 에러정정이 가능하도록 하는, 물리계층에서 콘볼루션 부호를 이용한 무선 센서 네트워크 보안 시스템 및 방법을 제공하는 데 그 목적이 있다.

과제 해결수단

<7> 상기와 같은 목적을 달성하기 위한 본 발명의 물리계층에서 콘볼루션 부호를 이용한 무선 센서 네트워크 보안 시스템은, 시스템이 요구하는 특정한 콘볼루션 부호 그룹을 선택받고, 상기 특정한 콘벌루션 부호 그룹 내의 콘볼루션 부호 생성 다항식 중, 특정 자유거리를 갖는 어느 일 콘볼루션 부호 생성 다항식을 선택받는 선택부; 상기 선택부에서 선택받은 콘볼루션 부호 생성 다항식을 보안키를 이용하여 랜덤하게 인터리빙하는 인터리버; 및 전송하고자 하는 정보비트를 상기 인터리버에서 인터리빙된 콘볼루션 부호 생성 다항식을 이용하여 인코딩하는 콘볼루션 인코더를 포함한다.

<8> 또한, 상기 선택부는, 상기 특정한 콘벌루션 부호 그룹 내의 콘볼루션 부호 생성 다항식 중 자유거리가 가장 큰 상계(上界)의 콘볼루션 부호 생성 다항식을 선택받고, 상기 인터리버는, 상기 선택부에서 선택받은 콘볼루션 부호 생성 다항식을 이진 형태로 배열한 행렬에 관한 행을 보안키를 이용하여 랜덤하게 인터리빙할 수 있다.

<9> 이 외에도, 상기 선택부는, 상기 특정한 콘벌루션 부호 그룹 내의 콘볼루션 부호 생성 다항식 중 자유거리가 가장 큰 경우인 상계(上界)에 근접한 자유거리를 갖는 어느 일 콘볼루션 부호 생성 다항식을 선택받고, 상기 인터리버는, 상기 선택부에서 선택받은 콘볼루션 부호 생성 다항식을 이진 형태로 배열한 행렬에 관한 행과 열을 보안키를 이용하여 랜덤하게 인터리빙할 수 있다.

<10> 한편, 상기 보안키는, 정보비트를 전송하는 소스 측의 정보 및 상기 콘볼루션 인코더에 의해 인코딩된 정보비트를 전송받는 목적지 측의 정보를 각각 조합한 것일 수 있다.

<11> 상기와 같은 목적을 달성하기 위한 본 발명의 물리계층에서 콘볼루션 부호를 이용한 무선 센서 네트워크 보안 방법은, 시스템이 요구하는 특정한 콘볼루션 부호 그룹을 선택받는 콘볼루션 부호 그룹 선택 단계; 상기 콘볼루션 부호 그룹 단계에서 선택된 특정한 콘벌루션 부호 그룹 내의 콘볼루션 부호 생성 다항식 중, 특정 자유거리를 갖는 어느 일 콘볼루션 부호 생성 다항식을 선택받는 생성 다항식 선택 단계; 상기 생성 다항식 선택 단계에서 선택받은 콘볼루션 부호 생성 다항식을 보안키를 이용하여 랜덤하게 인터리빙하는 인터리빙 단계; 및 전송하고자 하는 정보비트를 상기 인터리빙된 콘볼루션 부호 생성 다항식을 이용하여 인코딩하는 콘볼루션 인코딩 단계를 포함한다.

<12> 또한, 상기 생성 다항식 선택 단계는, 상기 특정한 콘벌루션 부호 그룹 내의 콘볼루션 부호 생성 다항식 중 자유거리가 가장 큰 상계(上界)의 콘볼루션 부호 생성 다항식을 선택받고, 상기 인터리빙 단계는, 선택받은 콘볼루션 부호 생성 다항식을 이진 형태로 배열한 행렬에 관한 행을 보안키를 이용하여 랜덤하게 인터리빙할 수 있다.

<13> 이외에도, 상기 생성 다항식 선택 단계는, 상기 특정한 콘벌루션 부호 그룹 내의 콘볼루션 부호 생성 다항식 중 자유거리가 가장 큰 경우인 상계(上界)에 근접한 자유거리를 갖는 어느 일 콘볼루션 부호 생성 다항식을 선택받고, 상기 인터리빙 단계는, 선택받은 콘볼루션 부호 생성 다항식을 이진 형태로 배열한 행렬에 관한 행과 열을 보안키를 이용하여 랜덤하게 인터리빙할 수 있다.

<14> 한편, 이러한 방법에서 상기 보안키는, 정보비트를 전송하는 소스 측의 정보 및 상기 콘볼루션 인코더에 의해 인코딩된 정보비트를 전송받는 목적지 측의 정보를 각각 조합한 것일 수 있다.

효 과

<15> 본 발명에 따른 물리계층에서 콘볼루션 부호를 이용한 무선 센서 네트워크 보안 시스템 및 방법은, 보안키를 이용한 생성 다항식의 랜덤 인터리빙에 의해 콘볼루션 부호화 기법을 이용하여 무선 센서 네트워크를 통해 전송되는 데이터의 비화 성능을 크게 향상시키며, 별도의 에러정정 데이터의 첨부나 장치 또는 알고리즘을 부가하지 않고서도 정보 데이터에 대한 에러 정정 능력을 자체적으로 갖출 수 있다.

<16> 또한, 본 발명에서는 무선 네트워크의 채널환경과 시스템의 요구 성능에 따라 데이터의 비화를 위한 구속장의 길이를 적정하게 조정하여 무선 랜(LAN) 환경이나 네트워크, 무선 이동통신 시스템 등의 다양한 무선 네트워크 시스템에 전반적으로 적용이 가능하다.

발명의 실시를 위한 구체적인 내용

<17> 이하 첨부된 도면을 참조하면서 본 발명에 따른 바람직한 실시예를 상세히 설명하기로 한다. 이에 앞서, 본 명세서 및 청구범위에 사용된 용어나 단어는 통상적이거나 사전적인 의미로 한정해서 해석되어서는 아니 되며, 발명자는 그 자신의 발명을 가장 최선의 방법으로 설명하기 위해 용어의 개념을 적절하게 정의할 수 있다는 원칙에 입각하여, 본 발명의 기술적 사상에 부합하는 의미와 개념으로 해석되어야만 한다.

<18> 따라서, 본 명세서에 기재된 실시예와 도면에 도시된 구성은 본 발명의 가장 바람직한 일 실시예에 불과할 뿐이고 본 발명의 기술적 사상을 모두 대변하는 것은 아니므로, 본 출원시점에 있어서 이들을 대체할 수 있는 다양한 균등물과 변형예들이 있을 수 있음을 이해하여야 한다.

<19> 도 1은 본 발명의 실시예에 따른 무선 센서 네트워크 보안 시스템을 이용한 송신블럭 구성도, 도 2는 본 발명의 실시예에 따른 무선 센서 네트워크 보안 시스템을 이용한 수신블럭 구성도, 도 3 내지 도 4는 도 1 또는 도 2에 이용되는 보안키 생성의 예시도, 도 5는 제안한 두 알고리즘의 오류율(BER: Bit Error Ratio) 성능 그래프, 도 6은 제안한 두 알고리즘의 보안 수준 비교 그래프이다.

<20> 기본적인 형태는 소스와 목적지 정보를 이용하여 콘볼루션 부호기에 각각 다른 생성 다항식을 선택하는 것이다. 그러나 콘볼루션 부호 생성 다항식의 모든 부호어가 좋은 성능을 가지는 것은 아니다. 더욱이, 콘볼루션 코드에서 특정한 부호는 불행의 부호로 불리며 매우 복잡한 다항식 선택을 발생시킨다.

<21> 따라서 본 발명에서는 보안 시스템 설계와 동시에 불행의 부호를 피하기 위한 알고리즘을 설계한다.

<22> 도 1에 도시된 바와 같이, 본 발명의 실시예에 따른 무선 센서 네트워크 보안 시스템(100)은 선택부(110), 인터리버(120), 콘볼루션 인코더(130)를 포함한다.

<23> 상기 선택부(110)는 시스템이 요구하는 특정한 콘볼루션 부호 그룹을 선택받고, 상기 특정한 콘벌루션 부호 그룹 내의 콘볼루션 부호 생성 다항식 중, 특정 자유거리를 갖는 어느 일 콘볼루션 부호 생성 다항식(실시예1; 자유거리가 가장 큰 상계(上界)의 콘볼루션 부호 생성 다항식, 실시예2; 자유거리가 상기 상계에 근접한 콘볼루션 부호 생성 다항식)을 선택받는 부분이다. 여기서 상기 선택부(110)는 키보드, 마우스 등과 같은 다양한 입력수단에 의해 가능할 수 있고 별도의 프로그래밍에 의해 가능할 수 있다.

<24> 다음으로, 상기 인터리버(120)는 상기 선택부에서 선택받은 콘볼루션 부호 생성 다항식을 보안키(Security Key)를 이용하여 랜덤하게 인터리빙하게 된다.

<25> 그리고, 상기 콘볼루션 인코더(130)는 전송하고자 하는 정보비트(Information Bits)를 상기 인터리버(120)에서 인터리빙된 콘볼루션 부호 생성 다항식을 이용하여 인코딩하는 부분이다.

<26> 이상과 같이, 본 발명에 따르면, 물리계층에서 랜덤하게 인터리빙된 '보안된 콘볼루션 부호 생성 다항식(Secured Generator Polynomial)'을 이용하여 상기 전송하고자 하는 정보비트를 인코딩함으로써, 물리계층에서 비화성을 증가시켜 원천 정보데이터의 보호가 가능하다.

<27> 또한, 상기 콘볼루션 부호를 통한 채널 부호화 기법을 이용함으로써, 전송채널에서 발생된 오류에 관하여 추후 수신측에서 완벽히 복구 가능한, 즉 에러 정정 기능이 가능한 이점이 있다. 즉, 별도의 에러정정 데이터의 첨부나 장치 또는 알고리즘을 부가하지 않고서도 정보 데이터에 대한 에러 정정 능력을 자체적으로 갖출 수 있다. 이는 콘볼루션 부호를 이용한 경우 일반적으로 에러 정정이 가능한, 콘볼루션 부호의 고유 특징에 해당될 수 있다.

<28> 한편, 상기 보안키란, 도 3 내지 도 4와 같이, 정보비트를 전송하는 소스(송신블럭 또는 송신기) 측의 정보(Source Information) 및 상기 콘볼루션 인코더(130)에 의해 인코딩된 정보비트를 전송받는 목적지(수신블럭 또는 수신기) 측의 정보(Destination Information)를 각각 조합한 것일 수 있다.

<29> 소스 측의 정보(Source Information)는, 소스ID(Source ID), 확산스펙트럼코드(Spread Spcetrum Code), 타임스케쥴(Time Schedule)로 구성된다. 또한 목적지 측의 정보(Destination Information)는 목적지ID(Destination ID), 확산스펙트럼코드(Spread Spcetrum Code), 타임스케쥴(Time Schedule)로 구성된다.

<30> 도 5는 상술한 소스 정보 및 목적지 정보를 서로 조합하여 완성된 보안키(Security Key;$S_1,S_2,\ldots,S_n,D_1,D_2,\ldots,D_n$)는, 추후 상기 인터리버(120)가 상기 선택부에서 선택받은 콘볼루션 부호 생성 다항식의 행(ROW), 열(COLUMN) 또는 행과 열을 랜덤하게 인터리빙하는데 이용된다.

<31> 한편, 상기 콘볼루션 인코더(130)에서 인코딩된 정보비트(Information Bits)는 무선통신이 가능하도록 변조기

(140)에서 변조된 후 안테나를 통해 송신 가능하다.

<32> 도 2는 이러한 시스템(100)을 이용한 수신블럭의 예를 나타내는 구성으로서, 도 1의 송신블럭 측으로부터 전송받은 신호를 복조기(160)에서 복조 및 검파한 이후, 암호화된 정보는 비터비 디코더(150)를 통해 복구되어 정보비트로 출력된다.

<33> 즉, 도 2의 선택부(110)는 도 1의 송신블럭에서와 동일 방식으로, 시스템이 요구하는 특정한 콘볼루션 부호 그룹을 선택받고, 특정한 콘벌루션 부호 그룹 내의 콘볼루션 부호 생성 다항식 중, 특정 자유거리를 갖는 어느 일 콘볼루션 부호 생성 다항식을 선택받는다.

<34> 그리고, 도 2의 인터리버(120)는 선택부(110)에서 선택받은 콘볼루션 부호 생성 다항식을 상술한 도 1의 동일 방식으로 보안키(Security Key)를 이용하여 랜덤하게 인터리빙한다.

<35> 상기 비터비 디코더(150)는 상기 인터리빙된 콘볼루션 생성 다항식을 이용하여, 복조기(160)로부터 전송받은 복조 신호의 암호화된 정보를 복구하여, 원신호인 정보비트(Information Bits)로 출력한다.

<36> 이하에서는, 이상과 같은 도 1의 시스템(100)에 관하여 두 가지 실시예를 들어 설명하고자 한다.

<37> [실시예 1]

<38> 첫 번째 실시예의 경우는 가장 좋은 성능 및 적절한 보안 수준을 보장한다.

<39> 여기서, 보안 수준의 증가는 부호율을 감소시킨다. 상기 성능이란, BER(Bit Error Ratio)를 나타내며 기존의 콘볼루션부호화 기법의 최고 성능과 동일하다.

<40> 코드의 선택 과정은 다음과 같다.

<41> - STEP1: 선택부(110)는 시스템이 요구하는 특정한 콘볼루션 부호 그룹을 선택받는다. 예를 들면 시스템의 요구에 따라, 구속장의 길이가 5이고 부호율이 1/4을 갖는 콘볼루션 부호 그룹을 선택받는다.

<42> - STEP2: 선택부(110)는 선택받은 콘벌루션 부호 그룹 내의 콘볼루션 부호 생성 다항식 중 자유거리가 가장 큰 상계(上界)의 콘볼루션 부호 생성 다항식을 선택받는다. 상기 구속장의 길이가 5이고 부호율이 1/4인 부호 그룹 중에서, 자유거리가 가장 큰 16을 갖는 상계의 생성 다항식 G는 아래 수학식 1과 같은 [25 27 33 37]이다.

<43> [수학식 1]

$$G = \begin{bmatrix} 25 \\ 27 \\ 33 \\ 37 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

<44>

<45> 이러한 G는 상기 상계의 콘볼루션 부호 생성 다항식을 이진 형태로 배열한 행렬을 나타내며, 자유거리(D_{free})는 16을 갖는다. 그리고 생성 다항식 G는 4개의 생성자(행성분)로 이루어져 있다.

<46> - STEP3: 인터리버(120)는, 선택부(110)에서 선택받은 상계의 콘볼루션 부호 생성 다항식을 이진 형태로 배열한 상기 행렬 G에 관한 행을 상기 보안키를 이용하여 랜덤하게 인터리빙하게 된다. 이렇게 랜덤 인터리빙된 콘볼루션 부호 생성다항식은 추후 상기 콘볼루션 인코더(130)에서 정보비트(Information Bits)를 인코딩하여 암호화하는데 이용된다.

<47> 이러한 첫번째 실시예는 구현이 간단하고 항상 가장 좋은 성능을 유지시킨다.

<48> STEP3에서는 행렬의 행성분만 랜덤 인터리빙되므로 인터리빙된 이후에도 생성 다항식 G는 D_{free}=16의 자유거리를 그대로 유지하며, 즉 4개의 생성자의 어떠한 조합이라도 선택된 콘볼루션 부호 그룹의 상계조건인 D_{free}=16의 자유거리를 갖는다.

<49> 4개의 생성자의 조합은 4!로서, 24가지의 경우의 수를 갖는다.

<50> 따라서 상기 행의 랜덤 인터리빙에 의해 생성 가능한 생성 다항식 행렬의 수는 24가지가 된다.

<51> 따라서, 비인증 노드가 받은 코드워드를 해독하기 위해 정확한 생성 다항식 그룹을 찾을 확률은 1/24로서 충분

히 낮다고 볼 수 있다.

<52> 일반적인 경우, 정확한 생성 다항식을 찾을 확률을 1/(1/R)!가 된다. 여기서 R은 부호율(본 실시예에서 R=1/4)을 나타낸다.

<53> 이 알고리즘은 R이 충분히 작다면 좋은 보안 수준을 제공할 수 있으나, 높은 부호율을 위한 보안 수준은 매우 낮아진다. 만약 1/2의 부호율인 경우는 해커나 비인증 사용자가 정확한 생성 다항식을 찾을 확률이 1/2!=0.5이므로 매우 높다.

<54> [실시예 2]

<55> 두 번째 실시예의 경우는 보안 수준을 높이기 위하여 약간의 성능 감소를 감안한 경우이고, 생성 다항식의 행과 열을 모두 인터리빙하여 높은 보안 수준을 얻도록 한다. 그러나 이러한 과정으로 인하여 나쁜 성능을 가지거나 Catastrophic 부호(불행의 부호)를 가질 수 있으므로 이러한 경우를 피하기 위해 다음과 같은 과정을 제안한다.

<56> - STEP1: 선택부(110)는, 시스템이 요구하는 특정한 콘볼루션 부호 그룹을 선택받는다. 예를 들면 시스템의 요구에 따라, 구속장의 길이가 5이고 부호율이 1/4을 갖는 콘볼루션 부호 그룹을 선택받는다.

<57> - STEP2: 선택부(110)는 선택받은 콘벌루션 부호 그룹 내의 콘볼루션 부호 생성 다항식 중 자유거리가 가장 큰 경우인 상계(上界)에 근접한 자유거리를 갖는 어느 일 콘볼루션 부호 생성 다항식을 선택받는다.

<58> 예를 들면, 상기 구속장의 길이가 5이고 부호율이 1/4인 부호 그룹 중에서, 가장 큰 자유거리를 나타내는 D_{free}=16과 근접한 자유거리를 갖는 D_{free}=14인 수학식 2의 콘볼루션 생성 다항식(G;[25 27 33 37])을 선택받는다.

<59> [수학식 2]

$$G=\begin{bmatrix}27\\33\\35\\37\end{bmatrix}=\begin{bmatrix}1&0&1&1&1\\1&1&0&1&1\\1&1&1&0&1\\1&1&1&1&1\end{bmatrix}$$

<60>

<61> 물론, 여기서도 이러한 G는 상계에 가까운 D_{free}=14인 콘볼루션 부호 생성 다항식을 이진 형태로 배열한 행렬을 나타낸다. 이 생성 다항식 G 또한 4개의 생성자로 이루어져 있다.

<62> 여기서 상기 생성 다항식의 선택 기준은, 불행의 부호를 피하기 위하여 전부 1인 '37'과 하나의 0을 포함하는 '33', '36', '27'을 선택하여 이루어지며, 자유거리는 14이다.

<63> - STEP 3: 인터리버(120)는, 선택부(110)에서 선택받은 콘볼루션 부호 생성 다항식을 이진 형태로 배열한 행렬 G에 관한 행과 열을 상기 보안키를 이용하여 랜덤하게 인터리빙한다. 이렇게 랜덤 인터리빙된 콘볼루션 부호 생성다항식은 추후 상기 콘볼루션 인코더(130)에서 정보비트(Information Bits)를 인코딩하여 암호화하는데 이용된다.

<64> 생성 다항식은 랜덤 인터리빙 되어 수학식 3과 같은 이진 행렬로 표현될 수 있다.

<65> [수학식 3]

$$G=\begin{bmatrix}33\\37\\36\\27\end{bmatrix}=\begin{bmatrix}1&1&0&1&1\\1&1&1&1&1\\1&1&1&1&0\\1&0&1&1&1\end{bmatrix}$$

<66>

<67> 즉, 수학식 2의 행렬에 포함된 3개의 0은 행렬을 구성하는 20개의 인수 중 어느 곳에도 배치 가능하다. 따라서 상기 행과 열의 랜덤 인터리빙에 의해 생성 가능한 생성 다항식 행렬의 수는 수학식 4와 같이 1140개가 된다.

<68> [수학식 4]

<69> $$\binom{20}{3} = \frac{20!}{(20-3)!\times 3!} = 1140$$

<70> 즉, 비인증 사용자에게 정확한 생성 다항식을 찾을 확률은 매우 낮은 1/1140의 확률이므로, 이 알고리즘에서 매우 높은 보안 수준을 제공할 수 있다.

<71> 이상과 같은 구성을 갖는 실시예 1 및 실시예 2의 알고리즘을 사용한 BER 시뮬레이션 및 분석 결과는 도 5 내지 도 6과 같다.

<72> 시뮬레이션에서는 위의 실시예1 및 실시예 2에서 사용한 부호들을 선택 이용하였다.

<73> 채널 환경으로는 레이리 페이딩(Rayleigh Fading) 채널과 AWGN(Additive White Gaussian Noise) 채널을 사용하여, 제안된 알고리즘의 BER 성능을 얻었다.

<74> 시뮬레이션에서는 위의 예에서 사용한 부호를 선택하였다. 또한 본 알고리즘과 동일하게 보안키를 이용하여 랜덤 인터리빙을 수행하였다. 그리고, 모든 데이터 전송 블록에서 보안키는 바뀐다고 가정하였다. 이것은 간단하게 PN코드나 시간의 함수를 이용할 수 있다.

<75> 도 5를 살펴보면, 실시예 2의 경우, 동일한 10^{-4}의 BER 성능에서 높은 보안 수준을 위해 실시예 1에 비해 약 1dB 정도 낮은 성능을 보인다.

<76> 도 6는 두 가지 알고리즘의 보안 수준을 비교한 것이다.

<77> 보안 수준(Security Level)은 BER성능을 로그 그래프가 아닌 상수 값으로 나타낸 것으로서, 에러 비트수를 전송 비트수로 나눈 값(Number of error bit/Number of bit))을 의미한다.

<78> 도 6을 보면, 실시예 2를 이용한 경우가 실시예 1의 경우에 비해 높은 보안 수준을 가지며. SNR 20dB에서 BER을 비교하여 보면 알고리즘 1은 0.391이고 알고리즘 2는 0.448이다. 두 알고리즘 모두에서 SNR값에 따른 BER값은 거의 일정하다.

<79> 이상과 같은 본 발명은 WSN에서 클러스터 헤더와 헤더 혹은 싱크가 서로 통신할 때 자신과 목적지의 정보를 이용하여 콘볼루션 부호화기법의 생성다항식을 랜덤 인터리빙함으로써 정확한 생성다항식을 만들어 내지 못하는 침입자로부터 비화성능을 향상시키도록 할 수 있다. 또한 물리계층의 프로토콜이므로 다른 통신시스템(예를 들면, 휴대전화, 군 통신, 휴대인터넷) 등의 대부분의 무선 통신환경에서 사용가능할 것으로 기대한다.

<80> 이상과 같이, 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 이것에 의해 한정되지 않으며 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 본 발명의 기술 사상과 아래에 기재될 청구범위의 균등 범위 내에서 다양한 수정 및 변형이 가능함은 물론이다.

도면의 간단한 설명

<81> 도 1은 본 발명의 실시예에 따른 무선 센서 네트워크 보안 시스템을 이용한 송신블럭 구성도,

<82> 도 2는 본 발명의 실시예에 따른 무선 센서 네트워크 보안 시스템을 이용한 수신블럭 구성도,

<83> 도 3 내지 도 4는 도 1 또는 도 2에 이용되는 보안키 생성의 예시도,

<84> 도 5는 제안한 두 알고리즘의 BER 성능 그래프,

<85> 도 6은 제안한 두 알고리즘의 보안 수준 비교 그래프이다.

<86> <도면의 주요 부분에 대한 부호의 설명>

<87> 100...무선 센서 네트워크 보안 시스템

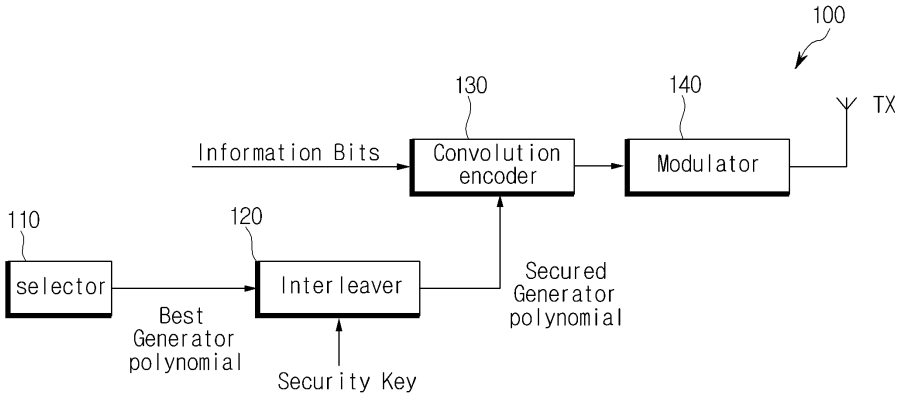
<88> 110...선택부 120...인터리버

<89> 130...콘볼루션 인코더 140...변조기

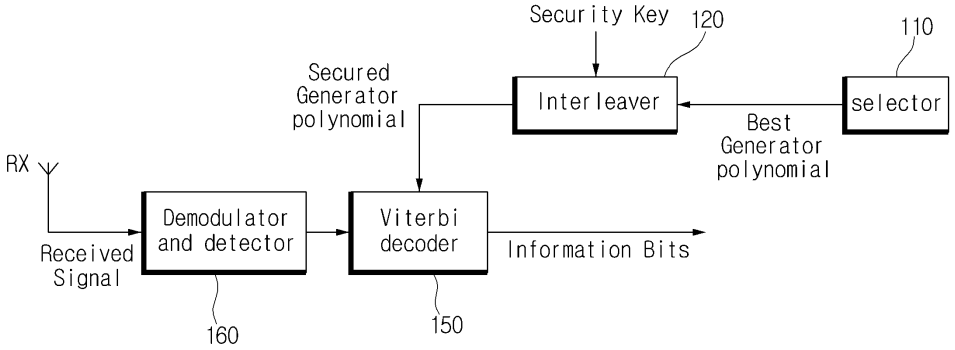
<90> 150...비터비 디코더 160...복조기

도면

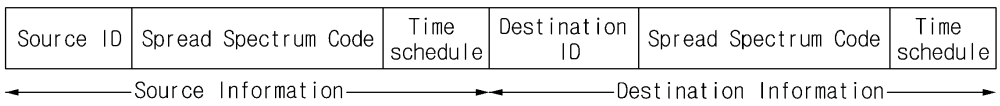
도면1



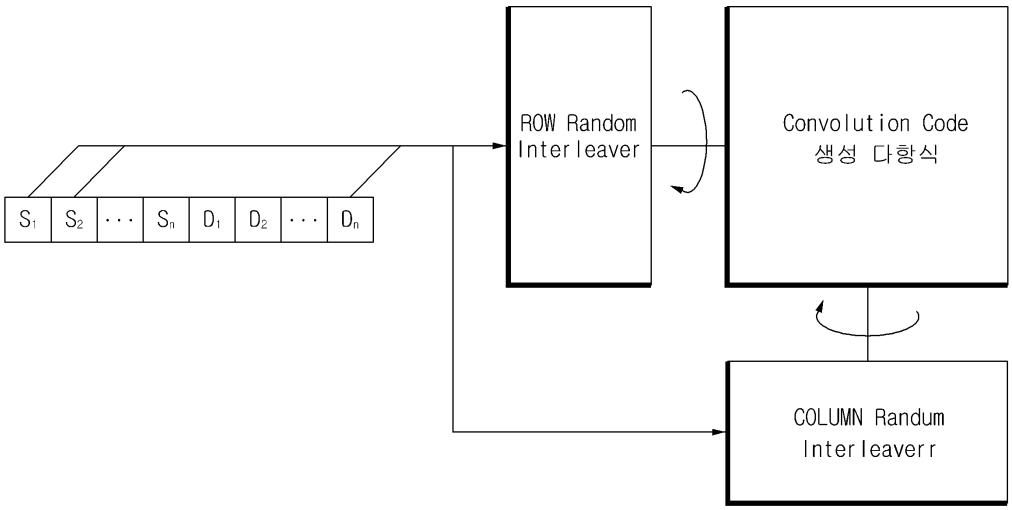
도면2



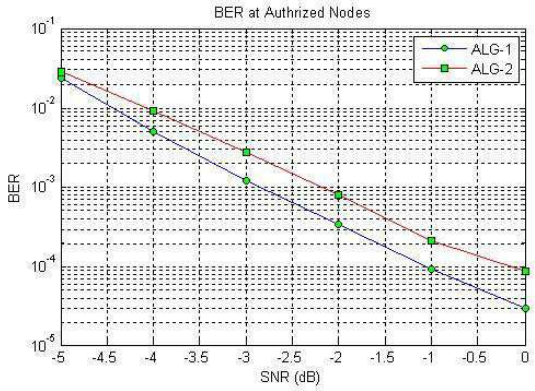
도면3



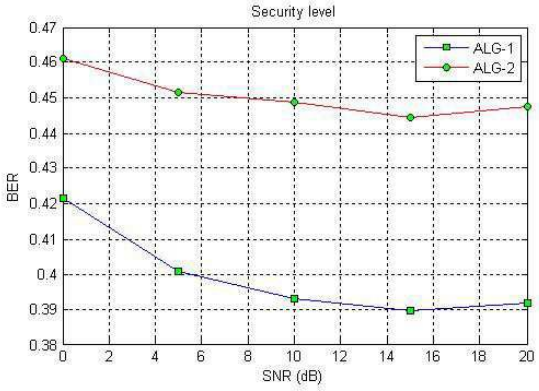
도면4


ROW Random
Interleaver
Convolution Code
생성 다항식
COLUMN Randum
Interleaverr
S1
S2
Sn
D1
D2
Dn

도면5


BER at Authrized Nodes
ALG-1
ALG-2
BER
SNR (dB)

도면6


Security level
ALG-1
ALG-2
BER
SNR (dB)