韓國通信學會論文誌 第16卷7號

論 文 要 約

91-55 : 일반화된 Diffie-Hellman 키이분배방식의 안정성 분석

李珊中 · 林采薰

본 논문에서는 관용 암호시스템을 위한 키이관리 방법으로 1976년 Diffie와 Hellman이 처음 제안한 유한체 상에서 이산대수 문제의 어려움에 바탕을 둔 공개 키이분배 방식(DH-KDS로 약칭)의 각종 변형들에 대해 그들의 안전성을 중점적으로 분석하여 보다 안전한 시스템을 설계하거나 설계한 시스템을 분석하는데 필요한 체계적인 접근법을 제시하고자 한다. 키이분배 방식에서 가능한 공격방법들을 분류하여 그들에 의해 깨어질 수 있는 시스템들을 기존 방식이나 설계 예를 통해 살펴봄으로써 이들을 피할 수 있는 방법들을 알아본다. 또한 안전성 분석의 도구로서 reducibility test나 정보이론적 접근법, 그리고 프로토콜 분석법 등을 소개하고 이들을 각종 DH-KDS의 변형들에 적용하여 그 안전성 여부를 검토한다.

91-56 : 복수 비직선 신호선로의 불요전자파 복사에 관한 해석

尹賢普 · 朴恒九 · 林桂在

단일 직선선로의 불요복사에 대한 이론을 확장하여, PCB와 같이 다수의 비직선 선로에 임의의 신호가 개별적으로 전송될 때 이 PCB 전체에서 발생하는불요전자파 복사의 크기를 정량적으로 구할 수 있는 보다 일반화된 해석방법을 얻기위하여 복사현상의 회로모형을 배열 안테나 이론에 적용하여 구했다.

제안된 해석방법의 타당성을 확인하기 위해 2개 및 3개의 서로 다른 임의의 비직선전송선로에 600MHz의 신호원을 인가하여 시뮬레이션한 결과와 측정된 불요복사 특성과 비교하여 서로 잘 일치함을 확인하였다.

91-57 : 신경회로망을 사용한 로보트 매니퓰레이터의 궤적 제어

安德煥 · 梁兌奎 · 李相孝

본 논문에서는 신경 회로망을 사용한 로보트 매니퓰레이터의 관절 궤적 제어 방법을 제안하였다.

매니퓰레이터의 역 동력학 모델을 신경 회로망을 통하여 학습시켜서, 그때의 신경 회로망의 가중치를 이용하여 매니퓰레이터를 제어한다. 가중치 값의 변화는 선형 제어기의 토크값 및 가속도 오차를 이용한다. 실제로 매니퓰레이터를 제어하는 토크값은 선형 제어기의 토크값과 신경 회로망 제어기 토크값의 합으로 된다.

컴퓨터 시뮬레이션을 통하여 제안된 제어 성능을 평가한다.

91-58 : The Dependence of the 1/f Noise on the Semiconductor Materials and Devices

Myong Ho SONG · Heui Jun PARK

In this paper the relative magnitudes of the 1/f noise constants were experimentally investigated in the plana type's resistors fabricated with the different type's semiconductor materials, and a new measurement technique for

the 1/f noise constant was suggested.

It was predicted from the experimental results that the origin of the 1/f noise in the semiconductor plana type's resistors may be located at the interface of the semiconductor and silicon dioxide.

91-59 : GaAs MESFET 모델 매개변수 추출에 관한 연구

朴義俊 · 朴鎭雨

GaAs MESFET 모델의 정확한 매개변수 값을 구하기 위하여 바이어스 의존성을 바탕으로 3가지 바이어스 변화에 대한 S-파라미터 측정만으로 모델 매개변수를 추출할 수 있는 새로운 계산 방법을 제시한다. Weighted Broyden updata 방법의 최적화 과정에서 얻어지는 오차 함수에 대한 매개변수의 감도를 이용해서 선형 및 비선형 매개변수의 유일해를 결정한다. 제안된 방법을 적용하기 위해 Marterka & Kacprzak 모델을 사용하였으며 추출한 매개변수 값의 정당성은 측정치와 비교함으로서 입증하였다.

91-60 : 最適 設計를 위한 3점 탐색 알고리즘의 제안

金周弘 · 孔徽植

最適 設計를 위한 최적치 탐색 알고리즘으로 直接 探索法의 일종인 3점 탐색 알고리즘을 제안하였다.

본 알고리즘은 N차원 탐색범위 내에 있는 數空間의 3^N점에서 함수의 최소치를 탐색하고, 점차로 탐색범위를 축소하여 동일한 탐색 과정을 반복 수행하는 방법이다. 그러므로, 1회 탐색시에 성능지표의 계산횟수는 3^N(N는 매개변수의 수)이다. 또한 3^N점 탐색법을 대신한 3N점에 대한 탐색법으로 단순 3N점 탐색법을 기술하였으나, 이것은 서로 다른 매개 변수가 乘除項을 갖는 성능지표의 경우에는 불확실함이 발견되었다.

제안된 알고리즘은 2차 형식이나 선형 함수로 구성되는 성능지표에 적용이 가능하며, 안정하고 신뢰도가 높은 특성을 갖고 있음이 확인되었다.

91-61 : 공개키 암호체계를 위한 Modular 곱셈개선과 통신회로구현에 관한 연구

韓善景 · 李先馥 · 劉泳甲

공개키암호화에 대한 지수계산 방법의 개선과 serial 통신선에 실용적으로 적용하는 방법을 제시한다. RSA형의 암호화 및 복호화 회로에 사용하기 위한 고속 modular 곱셈 알고리즘을 개선하였다. 기존의 고속 modular 곱셈 알고리즘에서 비교과정에 사용되는 control bit값 설정을 개선하여 부분곱과 modular값의 비교과정에서 오류가 발생되지 않도록 하였다. 이 개선된 알고리즘은 C 언어를 사용하여 작성한 simulation program에 의한 simulation을 통하여 그 정상 동작을 확인하였다. 또한 computer간의 serial 통신선에서 입력되는 serial data를 sampling하여 이것을 RSA 방식으로 암호화하여 송신하게 되고 수신측에서는 이의 역순으로 처리하며, 이 sampling 및 암호화에 Z80 microprocessor를 중심으로 암호회로를 설계 제작하였다.

91-62 : Noncoherent FSK DS/SSMA 통신의 다중 경로 다이버시티 수신 특성

安載泳 · 李在康 · 黃金燦

본 논문에서는 다중 경로 페이딩 채널에서 최대 다중 경로 지연폭이 한 비트 폭보다 큰 경우 발생할 수 있는 심볼간 간섭을 극복하기 위해 M-ary 신호방식과 절환 신호 방식을 채용한 다중 경로 다이버시티 수신 noncoherent FSK DS/SSMA 통신 시스템의 평균 오율을 평가하였다. 시스템의

평균 오율은 가우스 근사법을 이용해 채널 파라메타와 PN 시퀀스의 길이와 같은 시스템 파라메타에 대한 식으로 표현하였고, 이러한 결과식을 이용해 M-ary FSK 시스템과 두 종류의 절환 수신기에 대한 FSK 시스템의 평균 오율을 수치적으로 분석하였다.

91-63 : A Nonblocking Multi-Log$_2N$ Multiconnection Network : Theoretical Characterization and Design Example for a Photonic Switching System

Pil Joong LEE · Chae Hoon LIM

In this paper, the conditions on the number of required copies of a self-routing network with and without extra stages in back-to-back manner are presented respectively for a nonblocking multi-log$_2N$ multiconnection network. Actually the obained results hold regardless of connection patterns, i.e., whether a network deploys one-to-one connections or multiconnections. Thus open problems on the nonblocking condition for a multi-log$_2N$ multiconnection network are solved. Interestingly some of the given formulas comprise the Benes network and the Cantor network as a special case respectively. A novel switching system architecture deploying a distributed calls distribution algorithm is provided to design a nonblocking multi-log$_2N$ photonic switching network using a directional coupler. And a directional coupler based call holding demultiplexer is introduced to hold a call until blocking disappears in a switching network and let it enter to a network, provided that the number of switching networks is less than that of required switching networks for a nonblocking multilog$_2N$ network.