다중 반송파 DF 중계 네트워크의 향상된 물리계층 보안 전송 전략

이은지, 윤영준, 김성철
서울대학교 전기정보공학부
{ej9309, yyj0109, sckim}@maxwell.snu.ac.kr

A Physical-Layer Security Transmission Strategy in Multi-carrier DF Relay Network

Eunji Lee, Young-Jun Yoon, Seong-Cheol Kim
Department of Electrical and Computer Engineering, Seoul National Univ.

요 약

데이터 속도를 높이기 위해 사용하고 있는 다중 반송파 DF 중계 네트워크 시스템에서 최대 보안율을 얻기 위해서는 제한된 시스템 전력을 각 부반송파에 적절하게 할당을 해야 한다. 그러나, 최적 전력 할당 문제는 보안율이 전력에 대해 오목한 형태의 함수가 아니므로 최적화 문제로 풀 수 없고 전수조사를 통해 해를 구해야 하므로 계산량이 매우 크다. 이를 해결하기 위한 근사 전력 할당 방법 연구가 진행되고 있다. 이에 본 논문은 새로운 근사 전력 할당 방법을 제안하고 제안한 방법으로 보안율을 얼마나 달성할 수 있는지 시뮬레이션을 통해 검증하였다.

Ⅰ. 서 론

무선 통신은 전파를 방사하는 방식으로 통신하기 때문에 유선 통신에 비해 정보 보안 측면에서 취약하다. 기존 암호 기법으로 약속된 송신자와 수신자 간에 키를 이용하여 정보를 보호할 수 있지만, 도청자의 컴퓨터 연산 능력이 높아지면 무차별 대입 공격(brute-force attack)으로 보안을 뚫을 수 있다. 따라서, 도청자의 연산 능력에 의존하지 않고도 정보를 전송할 수 있는 보안 방식인 물리 계층 보안에 관한 연구가 진행되고 있다[1].

물리 계층 보안은 정보 이론을 기반으로 하는데 보안 정도를 나타내는 보안율(secrecy rate)은 송신자와 수신자 사이의 정보량에서 송신자와 도청자 간의 정보량을 빼 준 값으로 나타낼 수 있다. 보안율을 높이기 위해 데이터 속도를 높이는 방식을 취할 수 있지만, 단일 반송파 시스템에서 넓은 주파수 대역을 이용하면 심볼간 간섭(Inter-symbol interference, ISI) 문제가 발생한다. 데이터 속도를 높이면서 심볼간 간섭 문제도 해결하기 위해 직교주파수분할다중화(Orthogonal Frequency Division Multiplexing, OFDM) 시스템과 같은 다중 반송파 시스템을 이용해서 데이터를 전송한다. 이 경우, 각 부반송파 마다 겪는 채널이 달라진다. 각 부반송파에 의해 달성할 수 있는 보안율의 합을 최대 보안율이라 하고, 이를 높이기 위해 각 부반송파마다 전력 할당 및 전송 방식을 달리할 수 있다. 이렇게 다중 반송파 DF 중계 네트워크에서 총 보안율을 높이기 위한 부반송파 전력 할당에 관한 연구가 진행되어왔다. 그러나 총 보안율은 시스템에 할당된 전력에 대해 오목한(concave) 함수 형태가 아니므로 KKT 조건(Karush-Kuhn-Tucker conditions)을 이용하여 최적화 문제로 해결할 수 없다. 전수조사 형태로 최적해를 구할 수 있는데 부반송파의 개수가 늘어남에 따라 계산량이 기하적으로 증가한다. 계산량을 줄이기 위해 비오목(non-concave) 구간을 간단한 직선을 이용하여 오목 근사하여 근사해를 구하는 연구가 진행되었다[2].

이 방법에서는 전체 시스템 전력이 제한된 조건에서 부반송파 각각에 대한 분석을 통해 모든 부반송파의 보안율의 합인 총 보안율을 계산하였다. 그러나 각각의 부반송파에서 근사를 통해 통신 방식 결정한 후에 보안율을 계산하여 총 보안율을 구한 값은 전체 보안율의 관점에서 총 보안율을 계산한 값과 오차가 발생한다.

본 논문에서는 기존에 제시된 오목 근사의 결과로 나온 해보다 최적의 해에 더 근접하는 해를 구하는 기법을 제안한다. 제안 방법의 성능 검증을 위해 몬테-카를로 시뮬레이션을 이용하였다.

본 논문은 2장에서 시스템 모델과 제안 기법에 대해 설명하고, 3장에서 시뮬레이션 결과로 기존 기법과 성능을 비교한 뒤 4장에서 결론을 내린다.

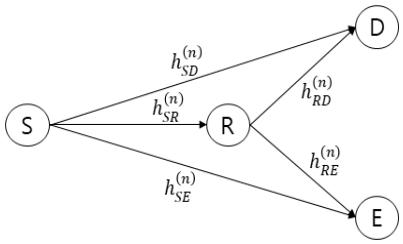


그림.1 다중 반송파 DF 중계 시스템 모델

Ⅱ. 본 론

2.1 다중 반송파 DF 중계 시스템 모델

본 논문에서는 그림 1과 같은 시스템 모델을 다루었다. 주파수 선택적 채널을 다루기 위해 각각 평탄한 페이딩을 겪는 N개의 직교 부반송파 시스템을 가정하였다. 반이중 전송 방식으로 전력을 할당하였으며, 첫 번째 시간 동안에는 송신자에만 전력을 할당하고, 두 번째 시간 동안에는 중계기에만 전력을 할당한다. 또한, 가산성 잡음(Additive Noise)은 평균이 0이고 분산이 σ^2인 상호 독립적인 복소 가우시안 랜

덤 변수로 가정하였다. 따라서 보안율은 다음과 같이 나타낼 수 있다 [3].

$$R_D^{(n)}(x) = \frac{1}{2}\log_2\left(\frac{\sigma^2+|h_{SD}^{(n)}|^2 x}{\sigma^2+|h_{SE}^{(n)}|^2 x}\right)$$

$$R_R^{(n)}(x) = \frac{1}{2}\log_2\left(\frac{\sigma^2+\frac{|h_{SR}^{(n)}|^2|h_{RD}^{(n)}|^2}{|h_{SR}^{(n)}|^2+|h_{RD}^{(n)}|^2-|h_{SD}^{(n)}|^2}x}{\sigma^2+\frac{|h_{RD}^{(n)}|^2|h_{SE}^{(n)}|^2+|h_{RE}^{(n)}|^2(|h_{SR}^{(n)}|^2-|h_{SD}^{(n)}|^2)}{|h_{SR}^{(n)}|^2+|h_{RD}^{(n)}|^2-|h_{SD}^{(n)}|^2}x}\right)$$

2.2 전력 할당 기법

전체 시스템 전력이 제한된 환경에서 특정 채널 환경에서는 할당된 전력이 작을 때에는 직접 통신 방식을 이용하다가 전력이 커짐에 따라 중계기를 이용한 통신 방식을 이용하는 것이 보안율을 높이는 경우가 있다. 반대로 중계기를 이용한 통신 방식을 이용하다가 할당 전력이 높아짐에 따라 직접 통신 방식을 이용하는 것이 보안율을 높이는 경우도 있다. 기존에 제안된 방법은 두 가지 경우(그림 2)에 대한 각각의 보안율의 기울기가 같아지는 두 지점을 직선으로 이어 비오목 함수를 오목함수로 만들어 KKT 조건을 이용한 최적화 문제를 푸는 방식이다. 이는 이러한 채널 환경에 해당하는 부반송파의 개수가 m개일 때, 최적 전력 할당을 위해 2^m번의 계산을 했던 것과는 달리 단 1번의 계산만을 요구한다.

본 논문에서 제안하는 방법은 할당된 전력이 직선 근사를 한 구간에 해당할 때에만 직접 통신 방식을 이용하는 것과 중계기를 이용한 통신 방식을 이용하였을 때 각각의 총 보안율을 계산해 더 높은 보안율을 달성하는 통신 방식을 채택하는 방법이다. 이는 기존에 제안된 방법보다 더 최적의 해에 근사한다.

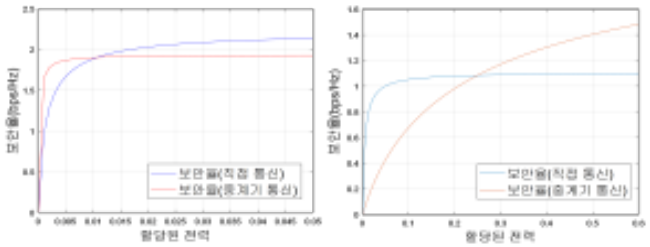


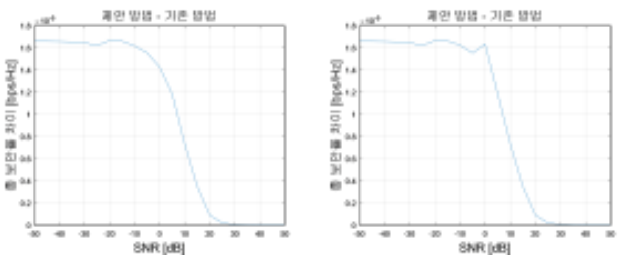
그림2. 할당된 전력에 따른 보안율

Ⅲ. 시뮬레이션

3.1 시뮬레이션 환경

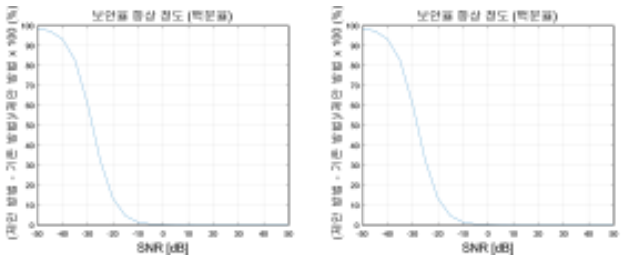
본 논문에서는 다중 경로를 고려한 COST207 전형적인 도시 환경 6-ray 채널 모델을 이용하였다. 경로 손실 지수는 일반적인 도시 환경에서 사용하는 값인 4를 이용했다. 송신자, 릴레이, 수신자, 도청자의 위치는 5×5 정사각형 환경에서 임의의 위치로 결정하였다. SNR은 -50 dB부터 50 dB까지 5 dB 간격으로 각 10000개의 채널을 설정하였다. NLOS (Non-line-of-sight) 환경은 송신자로부터 수신자, 도청자에 이르는 채널이 NLOS인 경우를 의미한다.

3.2 시뮬레이션 결과



(a) 임의의 채널 환경 (b) NLOS 환경

그림 3. SNR에 따른 기존 방법과 제안한 방법의 총 보안율 차이.



a) 임의의 채널 환경 (b) NLOS 환경

그림 4. SNR에 따른 제안한 방법의 보안율 향상 정도 백분율.

그림 3과 그림 4를 보면 임의의 채널에 대해 SNR이 감소할수록 기존 방법과 제안한 방법의 성능에 차이가 나타났다. 이는 시스템 전력에 대한 총 보안율 함수의 그래프가 로그 함수 형태로 나타나기 때문에 적은 전력에서 근사해를 구해야 하는 경우 최적 전력 할당으로 얻을 수 있는 보안율과 기존 방법으로 얻을 수 있는 총보안율의 오차가 크고, 제안한 방법이 이를 잘 보완해 줄 수 있음을 의미한다.

Ⅳ. 결 론

임의의 채널에 대해 SNR에 따른 본 논문에서 제안한 방법과 기존 방법의 총 보안율 차이가 항상 양의 값으로 나오는 것을 확인할 수 있다. 이는 제안한 방법이 항상 기존 방법에 비해 최적해에 더 근사한 값이라는 것을 알 수 있다. 또한, 제안한 방법은 기존 방법에서 근사해를 구하는 구간에서만 계산을 1번만 더 하므로 계산량은 많이 증가하지 않음을 알 수 있다. 특히 다른 채널보다 송신자에서 수신자나 도청자로의 채널이 NLOS인 경우에 SNR이 낮을수록 보안율 향상 정도가 컸다.

ACKNOWLEDGMENT

The research was supported by Samsung Electronics.

참 고 문 헌

[1] M Bloch, J Barros, “Physical-layer security: from information theory to security engineering,” Cambridge University Press, Sep. 2011.

[2] Cheol Jeong, Ill-Min Kim. “Optimal Power Allocation for Secure Multicarrier Relay Systems,” IEEE Transactions on Signal Processing, vol. 59, no. 11, pp. 5428-5442, Nov. 2011.

[3] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy", IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4005-4019, Sep. 2008.