다중 노드 네트워크에서 협력 중계와 인공잡음을 이용한 물리계층 보안 향상에 관한 연구

윤영준, 김진욱, 박정훈, 김성철

서울대학교

{yyj0109, kjwk9900, hoon0337, sckim}@maxwell.snu..ac.kr

A Study on the enhanced physical-layer security using cooperative relay and artificial noise in multiple intermediate node networks

Yoon Young-Jun, Kim Jinwook, Park Jeong Hoon, Kim Seong-Cheol

Seoul Nat'l Univ.

요 약

본 논문은 다중 노드 네트워크에서 물리계층 보안 향상을 위해 협력 중계와 인공잡음을 함께 이용하는 방안을 제안한다. 또한, 다중 노드 네트워크의 시스템 모델을 정의하고, 시스템 모델에서의 물리계층 보안 성능의 지표인 보안율 공식을 수립한다. 수립된 보안율 공식을 이용하여 협력 중계와 인공잡음을 위한 최적의 전력할당을 도출하고, 이를 제안된 물리계층 방안에 적용한다. 시뮬레이션 결과를 통해 기존 물리계층 보안 방안보다 제안된 방안이 성능을 보다 향상시킬 수 있음을 보여주었다.

Ⅰ. 서론

최근 5G 통신의 도래와 함께, IoT와 같은 다중 노드 네트워크 시스템이 차세대 통신 시스템의 중요한 패러다임으로 자리잡고 있다. 한편, 다중 노드 네트워크 시스템이 보다 접근이 용이해지고 사용자 친화적으로 진화함으로써 사용자의 개인적인 사적 정보가 네트워크에 노출될 가능성도 높아지게 되었다. 이러한 이유로 다중 노드 네트워크에서는 보안은 중요한 연구 주제로 다루어지고 있다. [1]

또한, 기존 암호화 보안 방식은 암호키 운용에 따른 높은 복잡성으로 인해 다중 노드 네트워크에서의 적용이 적절하지 않다. [2] 이에 암호키 운용을 필요로 하지 않는 물리계층 보안이 다중 노드 네트워크에서의 효율적인 보안 방식으로 각광받고 있으며, 암호화 보안 방식과 작동하는 계층이 다르기 때문에 간소화된 암호화 보안 방식과의 연동도 고려되고 있다.

본 논문에서는 다중 노드 네트워크에서 협력 중계와 인공잡음을 함께 이용하는 물리계층 보안 방안을 제안하고자 하며, 제안하는 물리계층 보안 방안을 위한 최적 전력할당도 같이 고려하고자 한다. 또한, 시뮬레이션 결과를 통해 제안된 물리계층 보안 방안이 기존 물리계층 보안 방안보다 보안 성능을 보다 향상시킬 수 있음을 보여주고자 한다.

Ⅱ. 본론

본 논문에서 고려하는 다중 노드 네트워크는 그림 1과 같다. 1개의 기지국 노드, N개의 중간 노드, 1개의 사용자 노드, 1개의 도청자 노드로 이루어져 있으며, h_{Bk}는 기지국 노드에서 k번째 중간 노드로의 채널을, h_{kD}와 h_{kE}는 각각 k번째 중간 노드에서 사용자 노드와 도청자 노드로의 채널 계수를 의미한다. 본 논문에서 제안하는 물리계층 보안 방안은 N개의 중간 노드 중 1개의 노드가 협력 중계 노드로 사용하고 나머지 N-1개의 중간 노드가 인공잡음을 위한 노드로 사용한다. 또한, 협력 중계 방식으로는 DF (Decode-and-Forward) 방식이 적용되며 N-1개의 중간 노드는 기지국 노드로 인공잡음이 방사되지 않도록 제로포싱 (Zero-forcing)의 협력 빔포밍 방식이 적용된다. 이에 더불어 기지국 노드의 전력 제한으로 인해 사용자와 도청자는 중간 노드들의 신호만 받는다고 가정한다. 이때, k번째 중간 노드를 중계 노드로 사용한다고 하면, 각각 사용자와 도청자가 받는 신호는 아래와 같다.

$$h_D = h_{kD}\sqrt{P_R}s + g_D \tag{1}$$

$$h_E = h_{kE}\sqrt{P_R}s + \vec{h}_{kE}^{T}\vec{w}_{kE}\sqrt{P_A} + g_E \tag{2}$$

h_D와 h_E는 각각 사용자와 도청자가 받는 신호이며, P_R과 P_A는 각각 중계와 인공잡음을 위해 사용되는 전력을 의미한다. 또한, $\vec{h}_{kE}$는 k번째 중간 노드를 제외한 나머지 중간 노드에서 도청자 노드로 향하는 채널 계수 벡터이며, $\vec{w}_{kE}$는 k번째 중간 노드를 제외한 나머지 중간 노드의 제로포싱 빔포밍 계수 벡터이다. g_D와 g_E는 각각 사용자 노드와 도청자 노드에서 수신되는 평균이 0이고 분산이 σ^2인 백색 가우시안 잡음이다. $(\bullet)^T$는 벡터 또는 행렬의 전치 (transpose) 연산자이다.

물리계층 보안의 성능 지표 중 하나인 보안율은 아래와 같은 공식을 따른다 [3].

$$R = [C_D - C_E]^+ \tag{3}$$

C_D와 C_E는 각각 사용자와 도청자의 채널 용량을 의미한다. 수식 (1)과 (2)를 이용하여 수식 (3)은 아래와 같이 변환 가능하다.

$$R_k = [\log_2\left(\frac{(1+\alpha_k P_R)(1+\gamma_k P_A)}{1+\beta_k P_R+\gamma_k P_A}\right)]^+ \tag{4}$$

α_k, β_k, γ_k는 각각 $|h_{kD}|^2$, $|h_{kE}|^2$, $|\vec{h}_{kE}^{T}\vec{w}_{kE}|^2$을 대신하며, R_k는 k번째 중간 노드를 협력 중계 노드로 사용했을 때의 보안율을 의미한다. (4)의 보안율 공식은 각각 P_R과 P_A에 대해 단조 증가 함수이므로,

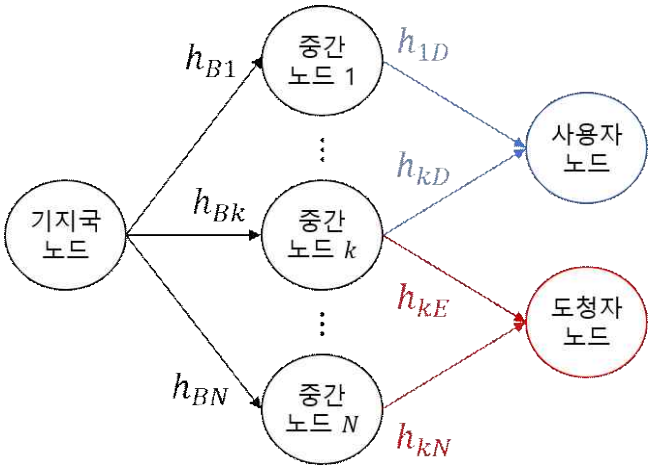

그림 1. 다중 노드 네트워크 모델

최적의 P_R과 P_A는 이들을 제한하는 해 가능 공간 (feasible set)의 경계에 존재할 수밖에 없다. 제안하는 물리계층 보안 방안에서 해 가능 공간의 경계는 아래와 같다.

$$|h_{Bk}|^2 P_S = |h_{kD}|^2 P_R \tag{5}$$

$$P_S + P_R + P_A = P_T \tag{6}$$

식 (5)는 DF 중계 방식의 중계 제한 조건에 의한 경계이며, 식 (6)은 전체 합 전력 제한 조건이다. P_T는 고려하는 네트워크에서 사용 가능한 최대 전력이다. 식 (5)와 식 (6)을 이용하면 식 (4)는 아래와 같이 변환된다.

$$R_k = \left[\log_2\left(\frac{(1+\alpha_k P_R)(1+\gamma_k P_T - \delta_k P_R)}{1+\beta_k P_R + \gamma_k P_T - \delta_k P_R}\right)\right]^+ \tag{7}$$

위 식에서 최적의 P_R은 R_k을 미분하여 얻은 미분식을 0으로 만드는 P_R을 찾음으로써 얻을 수 있으며, 이는 아래와 같다.

$$P_R^\star = \begin{cases} \dfrac{1+\gamma_k P_T}{\gamma_k - \beta_k}\left(1 - \sqrt{\dfrac{\beta_k}{\gamma_k}\left(1 + \dfrac{\gamma_k - \beta_k}{\alpha_k(1+\gamma_k P_T)}\right)}\right) & \text{for}\ \gamma_k \geq \beta_k \\ \dfrac{1+\gamma_k P_T}{\beta_k - \gamma_k}\left(\sqrt{\dfrac{\beta_k}{\gamma_k}\left(1 - \dfrac{\beta_k - \gamma_k}{\alpha_k(1+\gamma_k P_T)}\right)} - 1\right) & \text{for}\ \beta_k > \gamma_k \end{cases} \tag{8}$$

또한, 가능한 N개의 물리계층 보안 방안 중 최적의 물리계층 보안 방안은 아래와 같이 찾는다.

$$R^\star = \arg max_{\{k=1,2,\cdots,N\}} R_k(P_R^\star) \tag{9}$$

그림 2는 제안한 물리계층 방안의 성능과 기존의 협력 중계만을 사용하는 물리계층 방안의 성능을 비교한 그림이다. 총 10000번 반복의 몬테-카를로 시뮬레이션을 통해 보안율 성능을 도출하였으며, 중간 노드의 개수는 50개로 고정하였다. 본 그림을 통해 제안한 물리계층 방안의 성능이 기존의 협력 중계의 물리계층 방안 성능보다 향상됐음을 알 수 있다. 또한, 사용할 수 있는 최대 전력이 낮을 때에는 인공잡음을 사용하지 않고 협력 중계만을 사용하는 기존 방안이 최적 물리계층 보안 방안임을 알 수 있다. 하지만, 사용할 수 있는 전력이 점차 증가함에 따라 제안된 방안의 성능이 기존 방안의 성능을 추월하는 것을 볼 수 있는데, 이는 전력이 커질수록 인공잡음이 보다 효과적으로 도청자 노드에게 작용하여 사용자와 도청자의 채널 용량 차이를 크게 할 수 있다는 것을 의미한다.

Ⅲ. 결론

본 논문에서는 다중 노드 네트워크에서 보안 성능 향상을 위한 협력 중계와 인공잡음을 함께 사용하는 물리계층 보안 방안을 제안하였다. 또한, 네트워크 모델과 그에 따라 수립된 보안율 공식을 이용하여 최적의 전력 할당을 도출하였으며, 이를 제안한 물리계층 보안 방안에 적용하였다. 시뮬레이션 결과를 통해 제안한 물리계층 보안 방안이 기존의 물리계층 보안 방안보다 향상된 성능을 나타냄을 보였으며, 특히 전력이 커짐에 따라 성능 차이가 같이 커지는 것을 보여주었다. 추후에는 네트워크 모델에 다

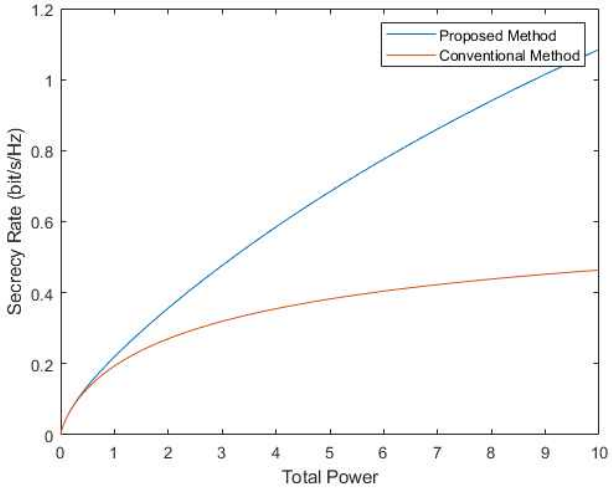

그림 2. 제안된 방안과 기존 방안의 전력에 따른 보안율 성능

중 부반송파 시스템을 함께 고려하여 OFDM과 같은 통신 시스템에 적용 가능한 물리계층 보안 방안을 연구해보고자 한다.

ACKNOWLEDGMENT

이 논문은 2021년도 두뇌한국21플러스사업에 의하여 지원되었음.

참 고 문 헌

[1] Lins, Fernando AA, and Marco Vieira. "Security Requirements and Solutions for IoT Gateways: A Comprehensive Study." IEEE Internet of Things Journal, pp. 8667-8679, November 2020.

[2] B. Schneier, "Cryptographic design vulnerabilities", Computer, vol. 31, no. 9, pp. 29-33, September 1998.

[3] A. D. Wyner, "The wire-tap channel," in The Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, October 1975.