다이버시티를 이용한 물리계층 보안기술 연구 동향

이동훈, 경연웅

공주대학교 정보통신공학과

mmdang@kongju.ac.kr, ywkyung@kongju.ac.kr

Research Trends of Physical Layer Security using Diversity

Lee Dong Hun, Kyung Yeun Woong

Div. of Inform. & Commun. Engineering Kongju National University

요 약

물리계층 보안기술은 무선채널의 물리적 특성을 활용하여 보완성능을 개선하는 기술로 기존의 보안기술의 대안으로 주목을 받고 있다. 이에, 본 논문은 최신 다이버시티(diversity)를 활용하여 보안성능을 개선하는 다이버시티 기반 물리계층 보안기술의 연구동향을 분석한다.

Ⅰ. 서 론

다이버시티(diversity)는 무선통신에서 송신기와 수신기 사이의 다양한 통신 경로를 의미한다. 다이버시티를 이용하여 통신성능을 개선하는 기술로 다중 송신안테나를 이용하여 다양한 통신경로를 확보하는 송신 안테나 다이버시티(transmit antenna diversity)기반 기술, 다중 수신안테나를 이용하는 수신 안테나 다이버시티(receive antenna diversity)기반 기술 그리고 다중 릴레이나 다중 사용자를 이용하는 노드 다이버시티(node diversity) 기반 기술이 있다. 또한, 2개 이상의 다이버시티를 동시에 이용하는 멀티 다이버시티(multi diversity)기반 기술이 있다.

Ⅱ. 본론

최신 다이버시티기반 물리계층 보안기술로 송신안테나 다이버시티기반 기술[1][2], 수신안테나 다이버시티기반 기술[3][4], 노드 다이버시티기반 기술[5]-[9] 그리고 멀티 다이버시티기반 기술[10]-[11]이 연구되었다.

[1][2]에서는 송신기는 다중안테나를 가지고 있고 수신기는 단일안테나를 적용하는 MISO(multiple-input single output) 시스템에서 다중 송신안테나를 이용하여 송신안테나 다이버시티를 증가시켜 보안성능을 개선하였다. [1]에서는 OTFS(orthogonal time frequency space) 시스템의 보안성능을 다중 송신안테나 중에서 채널 환경이 가장 좋은 안테나를 이용하여 데이터를 전송하는 전송안테나선택(transmit antenna selection) 기법을 이용하여 보안중지확률(secrecy outage probability, SOP) 성능을 개선하는 연구를 수행하였다. 성능분석결과 송신안테나 수에 비례하여 보안중지확률이 개선됨을 보였다. [2]에서는 주파수 공유를 하는 비직교다중접속(non-orthogonal multiple access, NOMA) 시스템의 보안성능을 수신기에서 심볼간 간섭을 제거하는 시공간블럭 코딩기법(space-time block coding, STBC)을 이용하여 보안중지확률과 보안용량(secrecy rate, SR)을 개선하는 연구를 수행하였다.

[3][4]에서는 송신기는 단일안테나를 가지고 있고 수신기는 다중안테나를 적용하는 SIMO(single-input multiple-output) 시스템에서 다중 수신안테나를 이용하여 수신안테나 다이버시티를 증가시켜 보안성능을 개선하였다. [3]에서는 디코딩 후 전달(decode and forward, DF)기반의 듀얼홉(dual hop) 시스템의 보안성능을 다중 수신안테나를 이용하는 MRC(maximal-ratio combining) 기법을 이용하여 보안신호포착확률(secrecy intercept probability, IP)을 개선하는 연구를 수행하였다. 성능분석결과 수신안테나 수에 비례하여 보안신호포착확률이 개선됨을 보였다. [4]에서는 차량통신을 위한 비직교다중접속 시스템의 보안중지확률과 보안용량 성능을 개선하는 연구를 수행하였다. 본 연구에서도 보안성능을 개선하기 위해 다중수신안테나 기반의 MRC 기법을 이용하여 차량통신의 보안성능이 수신안테나 수에 비례하여 개선됨을 보였다.

[5]-[9]에서는 다중 사용자나 다중 릴레이 중 채널 환경이 좋은 노드로 데이터를 전송하여 노드 다이버시티를 증가시켜 보안성능을 개선하는 연구를 수행하였다. [5]에서는 소스노드와 사용자노드 선택(pair selection)을 최적화하여 보안용량 성능을 개선하는 연구를 수행하였다. 본 연구에서는 주파수 선택 페이딩 채널 환경에서 순시 보안용량 값을 노드선택 기준으로 활용하여 노드 다이버시티를 개선하여 보안성능을 개선한다. [6]에서는 XL-MIMO(extra-large MIMO) 시스템에서는 보안용량을 극대화하는 사용자노드들을 스케쥴링(user scheduling)하고 선택한 사용자노드들의 데이터를 전처리(precoding)하여 전송하는 기법을 제안하였다. 사용자노드를 선택하는 기준으로 도청기의 수신 신호대 잡음비(leakage to interference plus noise, LINR)를 고려하였다. [7]에서는 주파수를 공유하는 비직교다중접속 시스템의 보안신호포착확률을 개선하는 연구를 수행하였다. 본 연구에서는 보안성능을 개선하기 위해 사용자노드 선택기법을 이용하였다. 기지국-사용자노드의 채널 이득과 기지국-도청기의 채널 이득의 차를 최대로 하는 사용자를 선택하는 사용자노드 선택의 기준을 제안하였다. 성능분석결과 사용자 노드 수에 비례하여 보안신호포착확률이 개선됨을 보였다. [8]에서는 1차 사용자와 2차 사용자가 주파수를 공유하는 환경에서 디코딩 후 전달 기반의 듀얼홉 시스템의 보안신호포착확률을 개선하는 연구를 수행하였다. 본 논문에서는 1차 사용자의 간섭채널 정보를 모르는 환경에서 적용가능한 릴레이 선택기법(non-interference aware relay selection, NIARS)과 1차 사용자의 간섭채널 정보를 알고 있는 환경에서 적용가능한 릴레이 선택기법(interference aware relay selection, IARS)을 제안하였다. NIARS기법은 릴레이 노드와 사용자 노드간의 채널이득을 선택기준으로 제안하였고 IARS기법은 보안용량을 선

택기준으로 제안하였다. [9]에서는 주파수 공유시스템에서 최적의 사용자 노드를 선택하여 상향링크(uplink) 보안성능을 개선하는 연구를 수행하였다. 최적의 사용자 노드 선택기법으로 사용자 노드와 기지국간의 채널 이득을 최대로 하는 사용자 노드를 선택하는 기법(selection combining, SC)과 threshold 값을 초과하는 사용자 노드를 선택하는 기법(switch and examine combine combining with post-selection, SECPS)을 적용하였다. [10][11]에서는 2개 이상의 다이버시티를 이용하는 시나리오를 고려하여 제안시스템의 보안성능을 개선하였다. [10]에서는 도청기가 다중 수신안테나를 이용하여 MRC와 SC 기법을 사용하는 환경을 고려하였다. 주파수 공유시스템의 1차 사용자의 보안성능을 개선하기 위해 전송 안테나선택 기법을 제안하였고 1차 사용자의 전송 안테나 선택을 위한 기준으로 기지국과 1차 사용자간의 채널 이득을 고려하였다. [11]에서는 송수신 안테나 다이버시티와 노드 다이버시티를 동시에 이용하여 증폭 후 전달(amplify and forward, AF) 시스템의 보안성능을 개선하는 연구를 수행하였다. 본 논문에서는 송수신 다이버시티를 얻기 위해 송신안테나 선택기법과 MRC 및 SC 기법을 제안하였고 노드 다이버시티를 얻기 위해 릴레이 및 사용자 노드 선택 기법을 제안하였다. 안테나 및 노드 선택 기준으로 순시 신호대 잡음비를 적용하였다.

Ⅲ. 결론

본 논문에서는 다이버시티를 이용한 물리계층 보안기술 연구 동향에 대해 분석하였다. 분석결과 송신안테나 다이버시티, 수신안테나 다이버시티, 노드 다이버시티 그리고 멀티 다이버시티 등 다양한 다이버시티를 이용하여 보안중지확률, 보안용량 그리고 보안신호포착확률 등 물리계층 관점에서 다양한 보안성능을 개선하는 연구가 활발히 수행되었음을 알 수 있었다.

참 고 문 헌

[1] Gunjan. G., Shrivastava S., and Kashyap S., "Modeling and analysis of physical layer security of OTFS systems under transmit antenna selection and passive eavesdropping," IEEE Comm. Lett.., vol. 28, no. 3, pp. 483-487, Mar. 2024.

[2] Li M., Bouanani F., Muhaidat S, and Dianati M., "Secure STBC-aided NOMA in cognitive IIOT networks," IEEE Internet of Things J., vol. 11, no. 1, pp. 1256-1271, Jan. 2024.

[3] Illi E., Qaraqe M., Bouanani F., and Kuwari S., "On the physical-layer security of a dual-hop UAV-based network in the presence of per-hop eavesdropping and imperfect CSI," IEEE Internet of Things J., vol. 10, no. 9, pp. 7850-7867, May. 2023.

[4] Jaiswal N., Pandey A., Yadav S., Purohit N., and Gurjar D., "Physical layer security performance of NOMA-aided vehicular communications over Nakagami-m time-selective fading channels with channel estimation errors," IEEE Open J. Veh. Technol., vol. 4, pp. 72-100, Apr. 2023.

[5] Kotwal S. Kundu C., Modem S., Dubey A., and Flanagan M.,. "Ergodic secrecy rate of optimal source-destination pair selection in frequency-selective fading," IEEE Trans. on Veh. Tech., vol. 72, no. 4, pp. 4598-4614, Apr. 2023.

[6] Anaya-Lopez G. Gonzalez-Coma J., and Lopez-Martinez F.,. "Leakage subspace precoding and schedulingfor physical layer security in multi user XL-MIMO systems," IEEE Comm. Lett.., vol. 27, no. 2, pp. 467-471, Feb. 2023.

[7] Li M., Yuan H., Cheng W., and Epiphaniou G.,"Physical layer security analysis of cognitive NOMA internet of things networks," IEEE Systems J., vol. 17, no. 1, pp. 1045-1055, Mar. 2023.

[8] Kong L., Yulong Z., and Li B.,,"Security and reliability tradoff of UAV relays assisted cognitive transmissions with hardware impairments," IEEE Internet of Things J., vol. 11, no. 6 pp. 10336-10351, 2024.

[9] Yan P., Ji X., Zou Y., and Li B.,"Securing multiuser underlay cognitive transmissions with hardware impairments and channel estimation error," IEEE Trans. Cogn. Commun. Netw., vol. 9, no. 5, pp. 1183-1199, Oct. 2023.

[10] Khoshafa M., Ngatched T., and Ahmed M., "RIS-aided physical layer security improvement in underlay cognitive radio networks," IEEE Systems J., vol. 17, no. 4, pp. 6437-6448, Dec. 2023.

[11] Lee D.,,"Secrecy rate TAS in AF-relay systems with multi-antenna relay and user over non-identical channel estimation error," IEEE Trans. on Veh. Tech., vol. 72, no. 3, pp. 2777-2788, Mar. 2023.