통합 감지 및 통신 네트워크에서의 다양한 보안 기법 조사

이충현, 오준석, 김재민, 백정엽, 조성래, 신용구*

중앙대학교, *고려대학교

{chlee;jsoh;jmkim}@uclab.re.kr, {jpeak;srcho}@cau.ac.kr, *ygssin92@korea.ac.kr

A Survey on Various Security Solutions for Integrated Sensing and Communications Network

Chunghyun Lee, Junsuk Oh, Jaemin Kim, Jeongyeup Peak, Sungrae Cho, Yonggoo Sin

Chung-Ang Univ., *Korea Univ.

요 약

최근 6G에서 핵심 기술로 대두되고 있는 통합 감지 및 통신(ISAC, Integrated Sensing and Communication)은 미래 6G 네트워크를 위한 최신 기술이다. 그러나 감지 파형을 통해 전달되는 메시지의 특성상 전파 방해(Jamming), 스푸핑, 도청 등의 보안 공격에 취약하므로 이로 인한 ISAC 네트워크의 보안 문제가 해결 과제로 제안되고 있다. 따라서, 본 논문은 최근 ISAC의 보안 문제를 해결하기 위한 연구를 조사하여 대표적인 보안 공격인 스푸핑과 도청 문제를 해결한 기술들을 소개한다.

Ⅰ. 서 론

다가오는 초지능형 시대에 요구되는 사항을 만족할 수 있는 차세대 6G 통신 및 네트워크에서는 기존에 제안되었던 공동 레이더 및 통신(JRAC, Joint RADAR and Communication)에서 확장된 Integrated Sensing and Communication에 관하여 많은 연구가 이루어지고 있다[1-2]. 특히, 다중 입출력(MIMO, Multi-Input Multi-Output) 안테나 모델, 지능형 반사 표면 (IRS, Intelligent Reflect Surface) 등 다른 핵심 기술들과의 융합을 기반으로 통신 속도 및 효율 측면에서 6G 네트워크 요구사항을 만족하는 장점을 나타내고 있다. 그러나, 일반적인 무선 통신의 보안 기술과 달리 감지 신호가 무선 통신 네트워크에서 무방비하게 노출되거나 쉽게 손실될 수 있는 특성 때문에 최근 ISAC 네트워크에서의 보안 솔루션을 제안하는 연구들이 급증하고 있다. 따라서, 본 논문은 대표적인 무선 통신 공격 기법인 스푸핑, 재밍, 도청에 대한 보안 솔루션을 제시한 연구들에 대하여 조사 및 분석을 실시한다.

Ⅱ. 본론

A. 스푸핑 및 재밍 공격 (Spoofing and Jamming Attack)

ISAC 기법은 6G 차세대 통신의 다양한 분야에 적용할 수 있으며, 특히 차량-사물(V2X, Vehicle-to-Everything) 간 네트워크에서의 지능형 교통 시스템을 구현하는 6G의 핵심 구성요소로 기대받고 있다. 온보드 센서에만 의존할 수 밖에 없는 자율주행에서 ISAC을 통한 높은 상황 및 자기 인식을 효과적으로 달성할 수 있다. 특히, GPS (Global Positioning System) 항법을 통해 안정성을 부가함으로써 기술 간 시너지를 극대화할 수 있다. 그러나, 민간 GPS 수신기의 암호화 및 인증 메커니즘이 취약한 경우 GPS 스푸핑 공격에 의해 복제된 위성 신호가 차량을 속이고 네비게이션 데이터를 조작하여 공격하기가 쉽다. 또한, V2X 링크는 공유 특성을 가지기 때문에 통신에 혼선을 주는 재밍 공격에도 취약하다는 단점을 가지고 있다. 이를 해결하기 위하여, [3]에서는 V2X 네트워크에서 GPS 스푸핑과 재밍 공격을 공동으로 탐지하여 방어할 수 있는 보안 솔루션을 제안하였다. 여러 차량에서 수신된 무선 주파수 신호와 해당 궤적 간의 상호 상관 관계를 통해 해당 신호가 복제 또는 조작된 것인지 판별한다. 특히, 상관 관계를 인코딩하는 동적 학습 모델을 제안하여 높은 효율을 나타내는 것을 시뮬레이션을 통해 확인할 수 있었다.

ISAC 네트워크에서의 보안 솔루션 연구는 재밍 공격에 대해서도 활발히 이루어지고 있다. [4]에서는 전파 방해 요소에 대해서, 통신과 재밍의 유사점을 검증하여 중첩된 파형을 오히려 통신의 강화 수단으로 사용하는 기법을 제안하였다. 통합 감지 및 재밍 (ISAJ, Integrated Sensing and Jamming)으로 명명된 프레임워크를 제안하여 기존의 ISAC과의 차이점을 비교 및 분석하고, 재밍을 보조하는 통신 및 통신을 보조하는 재밍을 포함한 시나리오를 통하여 실용성을 검증하였다. 최종적으로 ICAJ의 유효성을 검증하기 위하여 MIMO 기반 무선 통신 네트워크 환경에서 기존의 통신 및 감지의 분리 설계보다 ICAJ의 통신 및 전파 방해 성능이 보다 우수한 것을 검증하였다. 이를 통하여 통신과 전파 방해의 균형에 대한 실현 가능성을 제시하였으며, 균형이 이루어질 경우 기존의 분리 설계보다 보다 나은 성능을 가질 수 있다는 것을 확인하였다.

B. 도청 공격 (Evasdropping Attack)

ISAC의 취약한 보안 문제는 앞에서와 마찬가지로 감지 신호가 그대로 외부인에게 노출된다는 특성 때문이다. 즉, 감지 파형을 통해 전달되는 통신 메시지는 도청될 위험이 높다. 이를 해결하기 위하여 [5]에서는 보안을 보장할 수 있는 프리코딩 설계 기법을 통하여 도청 문제를 해결하였다. 뿐만 아니라 비직교 다중 접속(NOMA, Non-Orthogonal Multiple Access) 기반 ISAC 네트워크에서 보안이 보장된 최적화 문제를 해결할 수 있는 알고리즘을 제안하였다. Taylor 근사와 SOC (Second Order Convex) 제약 조건을 통하여 반복적으로 알고리즘을 수행하더라도 효과적인 최적화 솔루션과 보안 보장이 이루어지는 것을 시뮬레이션을 통해 확인할 수 있었다.

Ⅲ. 결론

본 논문에서는 최근 6G 보안 문제와 관련하여 대표적인 공격 방법인 스푸핑, 재밍, 그리고 도청에 대하여 ISAC 네트워크 모델에서의 보안 솔루션을 조사 및 분석하였다. 감지 신호가 무선 통신 네트워크에서 무방비하게 노출될 수 밖에 없는 특성을 고려하여 신호 뿐만 아니라 궤적 간의 상관 관계를 인코딩 및 학습하여 해당 신호의 진위 및 조작 여부를 판별할 수 있음을 확인하였고, 통신 전처리 단계에서 프리코딩을 보다 잘 설계하여 다중 접속 환경에서도 최적화와 더불어 보안 보장이 이루어 지는 것을 확인할 수 있었다. 뿐만 아니라, 재밍과 통신 간 유사점을 분석하여 통신 성능을 강화하는 통합 감지 및 재밍 기법을 제안하여 통신과 전파 방해 간 균형을 조절하는 것이 기존 대비 높은 효율을 시뮬레이션을 통해 검증하였다. 앞서 살펴본 보안 문제 이외에도 지속적으로 ISAC 네트워크 모델의 보안 문제를 면밀히 점검하고, 최종적으로 본 논문을 통하여 추후 연구에서는 ISAC 네트워크 모델을 구현할 때, 보안적인 문제를 같이 고려하여 차세대 6G 통신 및 네트워크 환경에 문제 없이 적용할 수 있을 것을 기대한다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업 (IITP-2024-RS-2022-00156353) 및 2022년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2022R1A4A5034130).

참 고 문 헌

[1] D. K. Pin Tan, J. He, Y. Li, A. Bayesteh, Y. Chen, P. Zhu and W. Tong, “Integrated Sensing and Communication in 6G: Motivations, Use Cases, Requirements, Challenges and Directions,” 2021 1st IEEE International Online Symposium on Joint Communications & Sensing (JC&S), 2021. Pp. 1-6, doi: 10.1109/JCS52304.2021.9376324.

[2] Q. Qi, X. Chen, C. Zhong and Z. Zhang, “Integrated Sensing, Computation and Communication in B5G Cellular Internet of Things,” in IEEE Transactions on Wireless Communications, vol. 20, no. 1, pp. 332-344, Jan. 2021, doi: 10.1109/TWC.2020.3024787

[3]] A. Krayani, G. Barabino, L. Marcenaro and C. Regazzoni, "Integrated Sensing and Communication for Joint GPS Spoofing and Jamming Detection in Vehicular V2X Networks," 2023 IEEE Wireless Communications and Networking Conference (WCNC), Glasgow, United Kingdom, 2023, pp. 1-7, doi: 10.1109/WCNC55385.2023.10118852.

[4] J. Gu, G. Ding, H. Wang and Y. Xu, "Integrated Communications and Jamming: Toward Dual-Functional Wireless Networks Under Antagonistic Environment," in IEEE Communications Magazine, vol. 61, no. 5, pp. 181-187, May 2023, doi: 10.1109/MCOM.002.2200538.

[5] Z. Yang, D. Li, N. Zhao, Z. Wu, Y. Li and D. Niyato, "Secure Precoding Optimization for NOMA-Aided Integrated Sensing and Communication," in IEEE Transactions on Communications, vol. 70, no. 12, pp. 8370-8382, Dec. 2022, doi: 10.1109/TCOMM.2022.3216636.