Optimizing Distributed Null-Steering as a Physical-Layer Security Technique in Over-the-Air Computation

Usman Iqbal, Haejoon Jung

Kyung Hee University

{usmaniqbal, haejoonjung}@khu.ac.kr

Abstract

This brief study extends previous work on physical layer security (PLS) using distributed null steering in over-the-air computation (AirComp) networks. While the original study derived closed-form expressions for mean squared error (MSE) and analyzed the secrecy performance, we further examine how the average MSE gap and the individual average MSEs at the legitimate receiver and the eavesdropper evolve under varying nulling factor. Simulation results demonstrate that increasing the nulling factor increases the average MSE gap, however, it significantly degrades the MSE at the targeted receiver. The results highlight the importance of optimizing nulling parameters to maximize secrecy without crossing the thresholds and performance constraints at the legitimate receiver. These findings offer deeper insight into the practical viability of the utilized PLS technique for enhancing AirComp network security.

Ⅰ. Introduction

The rapid proliferation of Internet-of-Things (IoT) devices requires efficient and secure data aggregation methods. Over-the-air computation (AirComp) is one of the most promising solutions, as it leverages the superposition property of wireless channels to compute functions like averages or weighted sums directly during the transmission process over the air [1]. However, there are serious concerns regarding information leakage to eavesdroppers, particularly in resource-constrained IoT environments.

Physical layer security (PLS) provides a less-complex alternative to traditional security methods by exploiting channel characteristics to keep the data secure from unauthorized receivers [2]. Recent work has explored distributed null-steering to enhance the PLS of IoT networks [3] and AirComp systems [4]. In particular, directing signal energy toward the intended receiver (Bob) while nulling in the vicinity of a potential eavesdropper (Eve) has proven effective in maximizing secrecy.

Previous work derived closed-form expressions for average mean squared error (MSE) and demonstrated that optimizing the nulling factor and direction significantly increases the MSE gap between Bob and Eve. However, the practical effects of varying the nulling factor on individual MSE values have not been fully characterized. In this work, we extend the prior analysis by investigating how varying nulling factor affect the average MSE at both Bob and Eve, as well as the MSE gap between them.

Ⅱ. System Model

As shown in Fig. 1, we consider a wireless AirComp system composed of U single-antenna sensor nodes transmitting data to Bob, while an Eve attempts to intercept the communication. At each transmission time interval (TTI), a subset of nodes is randomly selected to participate in data aggregation. The goal is to compute an arithmetic mean of sensor data at Bob via coherent superposition, while minimizing the information leakage to Eve.

The nodes are uniformly distributed over a circular area of radius R, and their positions are modeled in polar coordinates. Bob and Eve are both located in the far-field region, but with closely spaced angular locations, making Eve susceptible to intercepting the communication. Each node applies a beamforming coefficient that incorporates both channel-dependent scaling and a null-steering component aimed at data beamforming at Bob and degrading reception at Eve at the same time.

The nulling factor ε controls the trade-off between directing signal power toward Bob and introducing destructive interference in Eve's direction. A value of ε=0 corresponds to traditional analog cooperative beamforming (ACB), while ε=1 fully prioritizes null steering. The performance is measured in terms of the average MSE at both receivers and the average MSE gap, defined as the difference between average MSEs at Bob and Eve. The channel model assumes line-of-sight (LoS) conditions with phase shifts determined by the relative distances and angles. This paper evaluates using expressions in [4] through simulation to quantify how varying ε affects the balance between performance and security in realistic scenarios.

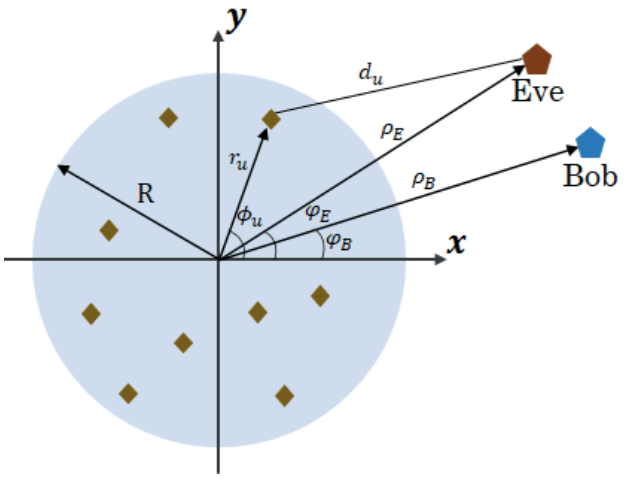

Fig. 1: System model for 2D AirComp-PLS

III. Simulation Results

For the simulation results, we utilized the same simulation parameters as [3]. The angular locations of Bob and data beamforming are same at 120^0, as well as, the angular locations of nulling and Eve are kept same 121^0. Fig. 2 shows the variation in MSE performance at different values of the nulling factor.

It can be observed that average MSE gap increases as we increase the nulling factor. The increase of the average MSE gap is desirable, however, one major issue is the change in the average MSE at Bob. It increases as well at higher values of nulling factor, degrading the reception at the desired location. Therefore, it is necessary to utilize an appropriate value for the nulling factor, so that it does not cross the desired threshold of the average MSE at Bob. For example, in the mentioned case, if the threshold is 0.01 for the average MSE at Bob, the maximum nulling factor that can be utilized is ~0.66.

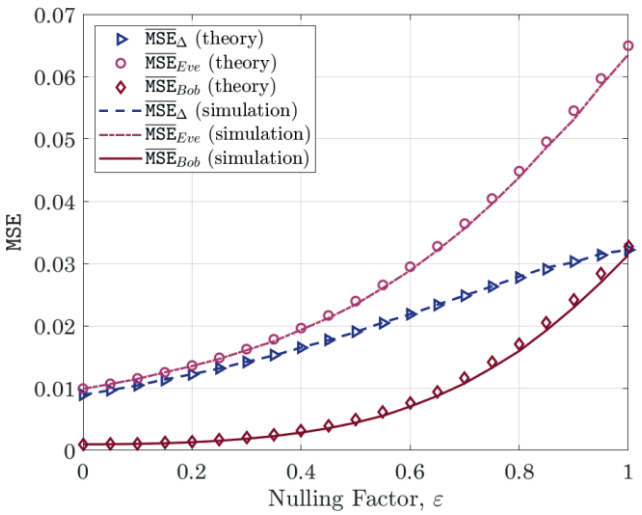

Fig. 2: AirComp MSE performance at different nulling factors

III. Conclusion

This study extends the research of physical-layer security in over-the-air computation (AirComp) networks by focusing on the impact of distributed null-steering techniques. It helps in identifying the trade-off between enhancing security and maintaining performance. Increasing the nulling factor increases the MSE gap, improving the secrecy, however it also deteriorates the MSE at the intended receiver, potentially violating quality of constraints. These findings provide valuable guidance for the practical applications of secure AirComp systems in resource-constrained IoT networks.

ACKNOWLEDGMENT

This work was supported by the MSIT, Korea, in part under the National Research Foundation of Korea grants (RS-2023-00303757), in part under the ITRC support programs (IITP-2025-RS-2021-II212046), and in part under the Convergence security core talent training business support program (IITP-2023-RS-2023-00266615) supervised by the IITP.

REFERENCES

[1] A. Ş ahin and R. Yang, "A Survey on Over-the-Air Computation," in IEEE Communications Surveys & Tutorials, vol. 25, no. 3, pp. 1877-1908, Third Quarter 2023.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," in IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1550-1573, Third Quarter 2014.

[3] H. Jung and I. -H. Lee, "Distributed Null-Steering Beamformer Design for Physical Layer Security Enhancement in Internet-of-Things Networks," in IEEE Systems Journal, vol. 15, no. 1, pp. 277-288, March 2021.

[4] U. Iqbal, S. Cho, H. Jung and M. Guizani, "Performance Analysis of Physical Layer Security for Over-the-Air Computation Using Distributed Null-Steering Beamforming," in IEEE Communications Letters, vol. 29, no. 2, pp. 303-307, Feb. 2025.