Cooperative Beamforming for Physical-Layer Security in Over-the-Air Computation

Usman Iqbal, Haejoon Jung, Hyundong Shin

Kyung Hee Univ.

{usmaniqbal, haejoonjung, hshin}@khu.ac.kr

Abstract

Over-the-air computation (AirComp) is a technique that enables the collection of desired function of data from a large number of nodes with limited available bandwidth. It utilizes the superposition property of the wireless channel that can be exploited to achieve the desired function of the sensors' data at the receiver. However, there is a possibility of a security attack on AirComp-based communication when an eavesdropper is located near the receiver. This article focuses on the utilization of cooperative beamforming to provide physical layer security (PLS) to the AirComp setup. The simulation results show that the use of cooperative beamforming increases the mean square error (MSE) in the vicinity of the receiver to counter security threats from eavesdroppers.

Ⅰ. Introduction

There has been rapid development of the Internet of Things (IoT) technology, which requires quick and efficient aggregation of the data in limited spectrum availability. Over-the-air computation (AirComp) is one of the best-emerging enablers to tackle this issue, as it utilizes the superposition property of the wireless channel to perform computations over the air, and the desired function of the sensing data is received at the desired location [1]. In the field of sensor networks, there are many applications where the exact data information from every sensor node is not required rather a function of all the measurements is needed [2] such as the average humidity level in a certain locality.

One of the main issues with wireless communication is its secrecy performance due to the possible eavesdropper receiving the transmitted information. Cooperative beamforming (CB) is one of the physical layer techniques (PLS) that assures secrecy against the eavesdroppers near the desired receiver [3]. In CB, the nodes transmit the data simultaneously by adjusting their phase in a way to target the desired angular direction.

This paper focuses on the utilization of CB with AirComp as a PLS technique to ensure secrecy performance. The performance comparison with no CB-based AirComp is investigated with mean square error (MSE) as the metric to show the secrecy improvement due to the proposed technique.

Ⅱ. CB-assisted AirComp

Figure 1 shows a 2D topology of an AirComp setup where there are K number of nodes located in a circular area of radius R from the origin O. Bob (the desired receiver) and Eve (an eavesdropper) are located in such a way that Eve is present near Bob. It is assumed that the receiver is located in the far-field, i.e., the distance between the Bob/Eve and the origin O is too large as compared to the radius R. The nodes transmit their data towards Bob simultaneously over a wireless channel, and the desired function of the data from the nodes is received at Bob. There are pre-processing functions (at Tx) and post-processing functions (at Rx) that are applied to achieve the desired function. Without any PLS technique employed, the data is vulnerable because of the possible eavesdroppers located near the desired receiver. The CB-based PLS technique provides a better secrecy performance near the receiver, as MSE increases at angular locations away from Bob.

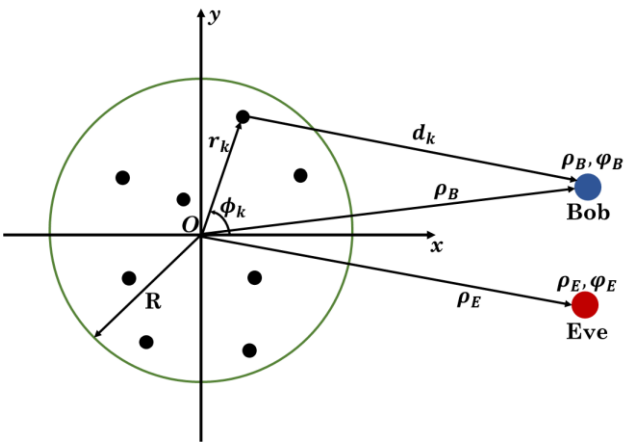

Fig. 1: System model for 2D AirComp

III. Simulation Results

For the simulation results, the parameters are listed in Table 1. The desired function at the receiver was the average function, and the Bob is assumed to be present at the angular location of 120^0. Fig. 1 clearly shows that utilizing CB as a PLS technique ensures a secure performance, as the MSE at Bob's location decreases significantly when CB is utilized. Furthermore, the employment of CB provides better MSE performance at Bob, and the MSE starts to increase as we move away from Bob.

Parameters	Values
Carrier Frequency	2 GHz
Number of Nodes, K	32
Radius (R)	10λ
Distance to Bob/Eve, ρ	1 km
Number of Frame Iterations	100,000

Table. 1: Simulation Parameters

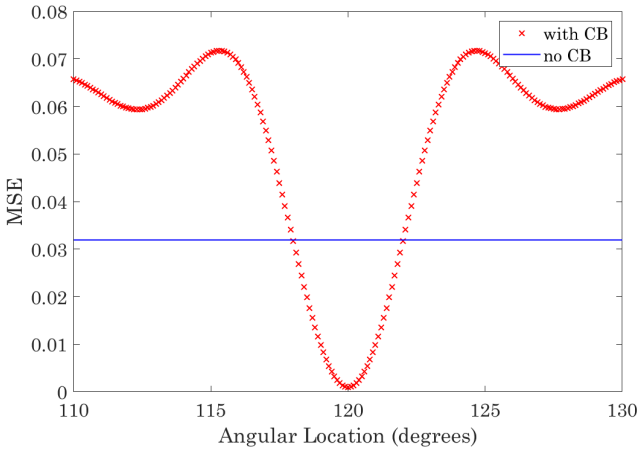

Fig. 2: AirComp MSE performance with and without CB

III. Conclusion

This article provided preliminary findings on utilizing CB as a PLS technique for AirComp. For a 2D network topology, the results were simulated for both cases, i.e., with CB and without CB. The results clearly show secure performance near the desired receiver. These results can be used as a platform for future research to further improve the PLS for AirComp.

ACKNOWLEDGMENT

This work was supported by the MSIT, Korea, in part under the National Research Foundation of Korea grants (RS-2023-00303757, NRF-2022R1F1A1065367 and NRF-2022R1A4A3033401) and in part under the Institute of Information & communications Technology Planning & Evaluation (IITP) grants (RS-2024-00397480, IITP-2024-2021-0-02046, IITP-2023-RS-2023-00266615).

REFERENCES

[1] H. Jung and S. -W. Ko, "Performance Analysis of UAV-Enabled Over-the-Air Computation Under Imperfect Channel Estimation," in IEEE Wireless Communications Letters, vol. 11, no. 3, pp. 438-442, March 2022.

[2] 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, thirdquarter 2023.

[3] H. Jung and I. -H. Lee, "Secrecy Performance Analysis of Analog Cooperative Beamforming in Three-Dimensional Gaussian Distributed Wireless Sensor Networks," in IEEE Transactions on Wireless Communications, vol. 18, no. 3, pp. 1860-1873, March 2019.