PROST: Privacy-Preserving and Truthful Online Double Auction for Spectrum Allocation

Abstract–

Spectrum auction is an effective way to redistribute scarce spectrum resources. However, most spectrum auction design only target at economic robustness, while neglecting the inherent privacy leakage problem. Existing secure spectrum auction mechanisms fail to provide adequate security, and they all neglect the online fashion of spectrum request arrival. In this paper, for the first time, we propose a Privacy-preserving and truthful Online double auction mechanism for Spectrum allocation in wireless networks, PROST. Compared with the state-of- the-art solutions, PROST provides a comprehensive and strong protection for users' sensitive information, especially for location privacy and time dynamics. PROST is constructed based on our carefully-designed security building blocks, which support various arithmetics over encrypted real numbers, and they are also well applicable in other spectrum auctions. Besides,we improve on existing online spectrum auction mechanisms by designing a novel privacy-preserving buyer grouping protocol for spectrum reuse. We not only theoretically prove thatPROST can realize an all-round security against semi-honest adversaries, but also extensively evaluate its performance. Experimental results validate that PROST achieves nice spectrum allocation efficiency with light computation and communication costs.

SHIELD TECHNOLOGIES

SHIELD TECHNOLOGIES,
2232, 3RD FLOOR, 16TH B CROSS, YELAHANKA NEW TOWN, BANGALORE-64
Mail us: shieldtechnoblr@gmail.com / manager@shieldtechno.com
Contact: 9972364704 / 8073744810