Underwater acoustic networked systems often consist of geographically distributed antenna elements (DAEs) that are connected via cables or high-rate radio links (e.g., bottom-anchored nodes or surface buoys). This paper investigates countermeasures against eavesdropping attack in the coordinated multipoint (CoMP) transmission of DAEs to an underwater legitimate user. Exploiting the low sound speed in water and the spatial diversity of DAEs, we propose signal alignment for transmission secrecy, where a transmission strategy will be judiciously designed such that useful signals will collide at the eavesdropper while stay collision-free at the legitimate user. Specifically, the transmit DAE set, and the transmission schedule and transmission power of each active DAE are jointly optimized with a goal of minimizing the maximal received signal-to-interference-and-noise ratio (SINR) of useful signals at the eavesdropper, under a lower bound constraint of the received signal-to-noise ratio (SNR) at the legitimate user. Taking the orthogonal frequency-division multiplexing (OFDM) as the modulation technique, simulation and emulated experimental results demonstrate that the proposed method significantly degrades the eavesdropper's interception capability. We further investigate the secrecy capacity and the secure degrees of freedom (d.o.f.) of the signal alignment method from an information-theoretic perspective, which reveals that without external helpers, secure d.o.f. greater than 1/2 can be achieved.