SECURE CONTINUOUS AGGREGATION IN WIRELESS SENSOR NETWORKS

Continuous aggregation is usually required in many sensor applications to obtain the temporal variation information of aggregates. However, in a hostile environment, the adversary could fabricate false temporal variation patterns of the aggregates by manipulating a series of aggregation results through compromised nodes. Existing secure aggregation schemes conduct one individual verification for each aggregation result, which could incur great accumulative communication cost and negative impact on transmission scheduling for continuous aggregation. In this paper, we identify distinct design issues for protecting continuous in-network aggregation and propose a novel scheme to detect false temporal variation patterns. Compared with the existing schemes, our scheme greatly reduces the verification cost by checking only a small part of aggregation results to verify the correctness of the temporal variation patterns in a time window. A sampling-based approach is used to check the aggregation results, which enables our scheme independent of any particular in-network aggregation protocols as opposed to existing schemes. We also propose a series of security mechanisms to protect the sampling process. Both theoretical analysis and simulations show the effectiveness and efficiency of our scheme.