Abstract

Sensor nodes deployed at hostile environments suffer compromise node attacks, in which an adversary injects counterfeit data into the sink causing error detection at upper level and energy wastage in en-route sensor nodes. A novel authentication scheme known as, Cooperative Bit-Compressed Authentication (CBA) is based on random graph characteristic of sensor node deployment and a cooperative bit-compressed authentication scenario with probability of neighboring nodes providing the necessary condition for CBA authentication. In this safest en-route is found out using client puzzle. Early detection and filtering of injected false data with CBA technique greatly saves energy adding a minor extra overhead at the en-route sensor nodes. The accompanied authentication information is bandwidth-efficient. Filtering of false data reduces the burden of the sink and in addition only very small fraction of injected bogus data needs to be checked by the sink. The high filtering probability, high reliability, throughput and energy saving of the CBA scheme is demonstrated in simulation results.

References

- Rongxing Lu. and Xiaodong Lin. , "BECAN: A Bandwidth-Efficient Cooperative

Index Terms

Computer Science

Wireless

Keywords