Abstract

In wireless sensor networks (WSNs), sensor nodes are vulnerable to false vote and false report injection attacks since they are widely deployed without infrastructure. Although some en-route filtering schemes can effectively detect the two attacks, these schemes need to set up various security factors before deploying the sensors in a sensor field. In this paper, we use a simulation model and find the proper security factors for a security scheme in a real-world simulation environment. We demonstrate that the scheme achieves better energy savings and detection power when the number of required message authentication codes (MACs) in a report is five and the number of detected MACs is two.

References

2. K. Akkaya and M. Younis, “A survey on routing protocols for wireless sensor networks,”


Index Terms

Computer Science

Wireless

Keywords

WSN, Voting-based Filtering, Discrete Event Modeling