



SURVEY ARTICLE

A Survey on Security Issues in Wireless Sensor Network

H.N. Pratihari

Department of Electronics & Communication Engineering
Centurion University of Technology & Management, Parlakhemundi- 761211
hnpratihari@rediffmail.com

Abstract— Sensor networks are key network to the creation of smart spaces, which embed information technology in everyday home and work environments. The miniature wireless sensor nodes, or motes, developed from low-cost off- the-shelf components at University of California, Berkeley, as part of its smart dust projects, establish a self- organizing sensor network when dispersed into an environment. The privacy and security issues posed by sensor networks represent a rich field of research problems. We consider routing security in wireless sensor networks. Many sensor network routing protocols have been proposed, but none of them have been designed with security as a goal. We propose security goals for routing in sensor networks, show how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduce two classes of novel attacks against sensor networks—sinkholes and HELLO floods, and analyse the security of all the major sensor network routing protocols. Improving network hardware and software may address many of the issues, but others will require new supporting technologies.

Key Terms: - WSN, Security; Network; Routing; Privacy

Full Text: <http://www.ijcsmc.com/docs/papers/July2013/V2I7201314.pdf>