Abstract

Several wireless sensor network applications ought to decide the intrinsic variance between energy efficient communication and the requirement to attain preferred quality of service (QoS) such as packet delivery ratio, delay and to reduce the power consumption of wireless sensor nodes. Also the intended protocols that are developed aims in providing better QoS with compromising security aspect. In order to address this challenge, we propose the Secured Power Aware Routing Protocol (PARP), which attains application-specified communication delays at low energy cost by dynamically adapting transmission power and routing decisions along with incorporating a novel cryptosystem. Through extensive simulation in NS2 the results prove that the proposed SPARP attains better QoS and reduced power consumption. Cryptool is used to test the novel proposed cryptosystem.

References

- Mark G. Simkin, &quot;Using Spreadsheets to Teach Data Encryption Techniques&quot;, AIS Educator Association, Volume 1, Number 1, pages 27 - 37, 2006.
- Osama Mahmud Abu Abbas, Khalid Mohammad Nahar, and Mohammad Ahmad Tubishat, &quot;Arae Cipher System&quot;, Computer Science Department, IT Faculty, Yarmouk University, Jordan, 2007.

Index Terms

Computer Science

Wireless Security

Keywords

Sensor networks  secured power aware routing  novel cryptosystem