Abstract

Since the time of their introduction, Wireless Sensor Networks (WSN) have been catching the interest of researchers. WSN have a wide range of applications, some even involving sensitive and secret information, thereby raising security concerns. Nevertheless, WSN have some constraints like limited memory, energy and computational capability, which pose an obstacle for the addition of proper security in sensor nodes. This paper introduces a new rekeying design for WSN security framework whose implementation would dispense effective security in the sensor nodes. This proposed security framework is endowed with the capacity to address security issues, such as message integrity, confidentiality, authenticity and freshness based on symmetric key cryptography. In addition, this design does not allow the storage of any key except the initial master key in the sensor nodes prior to network deployment. This paper also investigates reconfigurable sensor nodes in terms of execution time, memory, power consumption, and cost while running the security framework.
An Efficient Key Distribution Scheme in Wireless Sensor Architecture with Arduino and XBee


12.

Index Terms

Computer Science Wireless
Keywords

WSN, rekeying, security, symmetric cryptography