SECURING WIRELESS SENSOR NETWORKS USING CUSTOMIZED HARDWARE CRYPTO ENGINE

Lavanya Pathuri

Abstract

Wireless Sensor Networks (WSNs) are the original order of ad-hoc networks. They comprehend a complex linkage of self-determining sensor nodes that sense, measure and gather information from its remote environment. They send information congregated through wireless communications. WSNs are wireless, ad hoc, and unattended when deployed in the field of cognizance. They are vulnerable to security attacks by their broadcast nature in transmission, tiny battery, CPU power, and constrained memory capacity. Providing security in these systems is a challenge.

Research in providing optimal security to WSNs has made huge strides at a tremendous pace with security techniques. Cryptographic algorithms, which have been developed to impart security in traditional systems, have inappropriately proved themselves to be slow and power hungry in WSNs, when developed entirely in software. An alternative approach is to accelerate these algorithms by mapping them to customized hardware.

The objective of the research is to develop a power-efficient cryptosystem to provide the desired level of security on a smaller footprint, while maintaining real-time performance. Three algorithms have been selected to map them to hardware accelerators. These are Secure Hash Algorithm (SHA), Extended Tiny Encryption Algorithm (XTEA), and Advanced Encryption Standard (AES). These algorithms are profiled to understand their computational structure, which leads to better understanding of the performance bottlenecks. Then, hardware accelerators that describe these algorithms are prototyped to reconfigurable computing devices. Experimental results show speedup of up to 22x when compared to a software implementation of the algorithms running on contemporary CPU.