RADemics

Comparison of Energy Efficient Cryptographic Libraries for Wireless Sensor Networks

Piyush Charan, Dhivya S
MANAV RACHNA UNIVERSITY, VELALAR COLLEGE OF ENGINEERING AND TECHNOLOGY

Comparison of Energy Efficient Cryptographic Libraries for Wireless Sensor Networks

[1]Piyush Charan, Associate Professor, Department of Electronics and Communication Engineering, SOE, Manav Rachna University, Faridabad, Haryana, India. piyushcharan@mru.edu.in

[2]Dhivya S, Assistant Professor, Department of Computer Science and Engineering, Velalar College of Engineering and Technology, Thindal, Erode, Tamil Nadu, India. dhiviselva19928@gmail.com

Abstract

Wireless Sensor Networks (WSNs) have emerged as foundational components of modern cyber-physical systems, enabling large-scale data collection and intelligent decision-making across diverse domains such as environmental monitoring, healthcare, smart agriculture, and industrial automation. The integration of cryptographic protocols in WSNs was essential for ensuring data confidentiality, integrity, and authentication, the implementation of secure communication in these networks presents unique challenges due to stringent energy, memory, and computational constraints of sensor nodes. This book chapter offers a comprehensive analysis of energy-efficient cryptographic libraries tailored for WSN environments. It presents a comparative evaluation of lightweight cryptographic primitives, focusing on their performance, power consumption, and security effectiveness across various deployment scenarios. Special attention was given to the trade-offs between threat models and energy budgets, selection of primitives based on communication patterns such as broadcast and unicast, and the impact of network topology on cryptographic overhead, the chapter explores emerging strategies, such as hardware-software co-design and context-aware authentication, that aim to optimize cryptographic performance without compromising security resilience. The insights provided in this work serve as a foundational reference for researchers and system designers seeking to develop robust and energy-conscious security architectures in constrained WSN deployments.

Keywords: Wireless Sensor Networks, Lightweight Cryptography, Energy Efficiency, Secure Communication, Authentication Mechanisms, Cryptographic Libraries.

Introduction

Wireless Sensor Networks (WSNs) have emerged as a fundamental component in the architecture of modern intelligent systems, enabling the seamless integration of physical and digital environments [1]. Comprising spatially distributed autonomous nodes, WSNs are capable of sensing, computing, and communicating data across diverse applications such as environmental monitoring, industrial automation, healthcare, smart agriculture, and military surveillance [2]. These networks operate under significant constraints, including limited power supply, minimal processing capability, and reduced memory capacity [3]. Such constraints pose critical challenges in ensuring reliable and secure communication. The proliferation of WSNs in sensitive environments heightens the need for strong cryptographic mechanisms that can protect data against

a variety of threats without exhausting the finite energy reserves of the nodes [4]. Thus, embedding secure yet energy-efficient cryptographic protocols was essential for the long-term viability and trustworthiness of WSN-based systems [5].

Traditional cryptographic algorithms like RSA and AES, though widely used in general computing, often exceed the energy and processing limitations of WSN hardware [6]. These algorithms typically require extensive computation and larger memory footprints, which are unsuitable for battery-powered sensor nodes operating in remote or inaccessible locations [7]. The use of such algorithms can drastically shorten the operational lifespan of the network. Therefore, specialized lightweight cryptographic libraries have been developed to address these challenges [8]. These libraries are optimized to consume minimal power, utilize fewer CPU cycles, and occupy less memory space, making them more suitable for constrained environments [9]. The performance of these lightweight solutions must be thoroughly analyzed to ensure they do not compromise the security objectives while achieving energy efficiency [10].