Paper ID: 52726
student

52nd IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cyber-security threats to space missions and countermeasures to address them (4)

Author: Mr. Abeer Vaishnav
R V College of Engineering, Bengaluru, India, abeer.vaishnav13@gmail.com

Ms. Amulya M S
R.V.College of Engineering, India, amulya9498@gmail.com
Mr. Mardi Srikar
R V College of Engineering, Bengaluru, India, srikarmardi@gmail.com

COMPARISON OF SOFTWARE BASED VS. HARDWARE ACCELERATED AES-128 ENCRYPTION ALGORITHM FOR SECURE COMMUNICATION WITH NANOSATELLITES

Abstract

Security of the onboard systems is mandatory in order to prevent exploitation of any nanosatellite's control systems against unauthorized access, which may lead to fatal consequences. The paper describes the use of Hardware Accelerators specialized for real-time encryption of data, and a comparison between Software based vs. Hardware accelerated encryption by the implementation of AES-128 encryption standard. A strong encryption scheme is needed for security of the payload information of RVSAT-1 that consists of data generated from the onboard microbiological experiment. The AES-128 encryption standard requires a huge amount of time and computation power in order to be cracked and hence enhances the security of the data transmitted from the nanosatellite. The paper depicts a graphical trade-off study between encryption speedup, power consumed and throughput using both software based and hardware accelerated encryption techniques. The experiment is conducted using an integrated hardware accelerator for encryption, integrated into the onboard microcontroller. This is supposed to act as an additional microcontroller for the Telemetry, Tracking, and Command (TT&C) subsystem of RVSAT-1. The paper portrays the results of the aforementioned graphical comparison, depicting a greater performance boost in encryption with a comparably small increment in the power consumption. It also emphasizes on the importance of using integrated hardware accelerators for encryption of data in nanosatellites.