An AES Cryptosystem For Small Scale Network

Ukrit Arom-oon
Control and Communication Division
Defence Technology Institute
Pakkret, Nonthaburi, Thailand
ukrit.a@dti.or.th

Abstract—**The Advanced Encryption standard (AES) cryptosystem for the small scale network presents the implementation of the AES algorithm, FIPS 197, on the microcontroller operated on the real-time operating system (RTOS) for securing data in a small scale network for example as an UAVs wireless communication. The Electronic Code Book (ECB) mode of the AES algorithm is mainly used as the cryptographic core. The RTOS has a scheduler with Pre-emptive scheduling algorithm in which each role is to give access the processor for tasks with higher priority. The target hardware is implemented on the arm cortex-M4. The performances of the implemented system are evaluated based on the communication of UAVs including the control commands and telemetry commands.**

Keywords—**AES, RTOS, FIPS, ECB, RTOS, AES-128, AES-192, AES-256, UAVs command**

I. Introduction

The new Advanced Encryption Standard (AES) selected from the Rijndael algorithm was announced as the new cryptographic algorithm, named for Advanced Encryption Standard (AES) (FIPS PUB 197), by the Federal Information Processing Standards (FIPS) in order to replace the old Data Encryption Standard (DES) in November 2001 [1]. The main characteristic of AES is a symmetric block cipher that can encrypt and decrypt information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext convert the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

Wireless applications in small scale networks such as reading sensors in wireless sensor network or the UAV-C2 data link in which data from a source to a destination are protected with cryptographic processes have commonly used the wireless module equipped with the cryptographic part. The zigbee module is an example of the module possessed an AES cryptographic part, but the module is limited with AES 128-bit-key encryption algorithm [2]. The FIPS 197 is the data encryption algorithm to protecting data to thwart malicious attacks as recommended by [3].

The AES algorithms are widely implemented in FPGAs and compare to different hardware implementations. [4] is an example of implementation AES on the different FPGA hardware and techniques. FPGAs perform fast in encrypting data even in complexed algorithms; the complexities. The current microcontroller capabilities are fast and can process the instruction within one cycle. There are some security applications used microcontrollers to implement the security system such as [5] and [6]. The performance of MCU by [5] shows that the RSA 1024-bit are encrypted within 82.2 microseconds with 8-bit microcontroller ATMEGA 2560 in the Arduino R3 platform with the peripheral java card.

In the encryption processes, the microcontroller must have run many tasks such as transceiving information, encrypting information, decrypting information and communicating with other peripherals of the MCU. In this case, the time constraint and the reliability are important in which the MCU must process the entire tasks simultaneously in time. Generally when the time constraint and the reliability are important, most of control systems use now real-time operating systems (RTOS) to ensure temporal constraint and reliability. RTOSs are widely used in most common systems like internal calculators of vehicles, nuclear power plants, telecommunications system, etc. [7]. Most complex real-time systems require a number of tasks to be processed independently and this require some scheduling task control mechanism [8].

This paper will study what performances of AES algorithm running on the RTOS for microcontrollers are, and the contribution by running with emulated-UAV-communication parameters such as UAV messages, message size, message rate, etc.

II. Background

A. Advanced Data Encryption(AES)

The AES algorithm described by [1] is a systematic block cipher that can encrypt (encipher) and decrypt (decipher) data in a block of 128 bits represented by **Nb** = 4, and the cryptographic key length128, 192 and 256 bits represented by **Nk** = 4, 6 and 8 respectively. The number of rounds for the cipher or decipher is depended on the key length **Nr** = 10, 12 and 14 for the **Nk** = 4, 6 and 8 respectively. The cipher and decipher start when the plain text or the cipher text is stored in the input array, and is arranged by the array of bytes, in0, in1,..., in15 orderly. After arranged data in the Input array is copied to the State array for Ciphering or Deciphering. The final state is copied the array of bytes from the State array to the Output state array that is the cipher text or plain text depending on the Input array. The AES algorithm is illustrated in Fig. 1.

The AES round transformation algorithm applied for both the cipher and the inverse cipher uses a round function that is composed of four different byte-oriented transformations.