SETSCI Conference Indexing System,
Volume 2 (2018), 153-153

ISAS 2018
I[st] International Symposium on Innovative Approaches in Scientific Studies
April 11-13, 2018, Kemer-Antalya, Turkey

Comparing the Performance of Encryption Algorithms in ZigBee Based Wireless Sensor Networks

Cebrail Çiflikli[1*], Kadir Aba[2*]
[1]Kayseri Vocational School, Erciyes University, Kayseri Turkey
[2]Vocational School, Nevşehir Hacı Bektaş Veli University, Nevşehir Turkey
[*]Corresponding author: aba@nevsehir.edu.tr
[+]Speaker: aba@nevsehir.edu.tr
Presentation/Paper Type: Oral / Abstract

Abstract- Wireless Sensor Networks, used widely nowadays, are likely to be unprotected against a variety of external attacks because they are often used in outdoor applications. Protecting the network against attack and ensuring the safety of the data has always been important for Wireless Sensor Networks. Encryption algorithms and data encryption methods are used to make communication secure.

In the study, it is aimed to test the performance of different encryption algorithms on resource-constrained wireless sensor networks and to determine the most suitable for wireless sensor networks. The performances of 9 (RSA, DES, AES, TEA, XTEA, RC4, RC5, BlowFish and Shamir Secret Sharing) encryption algorithms in wireless environment are compared in terms of encryption, decoding, transmission times, data sizes and energy parameters they used.

To compare the algorithms, a ZigBee-based wireless network environment consisting of wireless receiver and transmitter is prepared. The processes are run using the Atmega 2560 microprocessor.

As a result of the study, it was determined that the compared algorithms had superiority to each other in different fields. Based on the total processing time of encryption, data transmission and decryption stages, the most appropriate algorithm for Wireless Sensor Networks is determined.

Keywords- Wireless Sensor Networks, ZigBee, Security, Encryption