The Best Performance Evaluation of Encryption Algorithms to Reduce Power Consumption in WSN

Mustafa A. Al Sibahee, Songfeng LU
School of Computer Science and Technology
Huazhong University of Science and Technology, Wuhan, 430074, China
Email: MUSTAFA.A@hust.edu.cn, lusongfeng@hust.edu.cn

Zaid Alaa Hussien
Southern Technical University, Basrah, Iraq

Mohammed Abdulridha Hussain, Keyan Abdul-Aziz Mutlaq, Zaid Ameen Abduljabbar
University of Basrah, Basrah, Iraq

Abstract— **Wireless Sensor Networks (WSNs), applications are growing rapidly, so the needs to protect such applications are increased. Cryptography plays a main role in information system security where encryption algorithm is the essential component of the security. On the other side, those algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. This paper provides evaluation of four of the most common encryption algorithms namely: RC4, DES, and AES as a symmetric cipher and RSA for asymmetric cipher. A comparison has been conducted for those encryption algorithms at different settings such as different sizes of data blocks, different key size and finally encryption/decryption speed. Simulation results are given to demonstrate the effectiveness of each algorithm on power consuming.**

Keywords- Encryption techniques, power consumption, WSN security.

I. INTRODUCTION

Wireless sensor networks (WSN) are used to monitor environmental and physical changes by means of sensor nodes[1]. Which are becoming a popular ubiquitous computing. They are used in different applications such as health care monitoring, environmental/earth sensing, air pollution monitoring, forest fire detection, industrial monitoring and many more. Since there are only limited resources, WSNs are exposed to many vulnerable attacks such as false message injection, eavesdropping etc., hence more security measures are needed. In recent times many techniques such as random key pre-distribution and random pairwise key distribution has been used. The security in WSN has been enhanced by using a symmetric key encryption technique. The pros and cons of the issues related to WSN have been put forth discussed, compared and evaluated in this research. Cryptographic is a set of algorithms operate in a way to encrypt and decrypt data. Encryption is transform plaintext to cipher text to serve security purposes. Whereas decryption is transform cipher text to plaintext that is the reverse operation of the encryption. Cryptography is divided in to two main category symmetric and asymmetric algorithms. Symmetric is using a same key for encryption and decryption by both sender and receiver .The challenge is how to security shared the key between the pairing nodes. WSN method for key distribution is by saving the key using offline phase , in other words , storing the key before the node operate . The drawback of this method is the static key value .while symmetric is preferred because low cost and high speed computation [5].

In order to optimize the conventional security algorithms for WSNs, it is necessary to be aware about the constraints of sensor nodes [2]. The major constraints of a WSN are Energy constraints. Energy is the biggest constraint for a WSN. In general, energy consumption in sensor nodes can be categorized in three parts: (i) energy for the sensor transducer, (ii) energy for communication among sensor nodes, and (iii) energy for microprocessor computation. According to the study in [3].one bit transmit with in WSN media will consumes power more than execution about 800 to 1000 instruction in WSN node. The consolation from such study is lead to reduce the communication messages size to save energy.

Security message data may results increasing data size spirally when using complex cryptography algorithms such as PKI. As mentioned above complicated mechanisms will directly effects the system power consuming.

The objective in this Paper is presenting varies security methods from power consuming point of view and the main contribution in WSN field as follow:

- We demonstrate the relationship between different security algorithm and power consumption.
- We measured the execution times for nods communication when using different security algorithms to recognize the best security algorithms to prolong power consumption.
- The affrication of distance between nods on power is presented in our work.

978-1-5386-3886-6/17 $31.00 © 2017 IEEE
DOI 10.1109/CIIS.2017.50