Available online at www.sciencedirect.com

ScienceDirect

Journal of Electrical Systems and Information Technology 2 (2015) 296–313

www.elsevier.com/locate/jesit

Two-phase hybrid cryptography algorithm for wireless sensor networks

Rawya Rizk *, Yasmin Alkady

Electrical Engineering Department, Port Said University, Port Said, Egypt

Received 25 May 2015; received in revised form 25 November 2015; accepted 25 November 2015
Available online 8 December 2015

Abstract

For achieving security in wireless sensor networks (WSNs), cryptography plays an important role. In this paper, a new security algorithm using combination of both symmetric and asymmetric cryptographic techniques is proposed to provide high security with minimized key maintenance. It guarantees three cryptographic primitives, integrity, confidentiality and authentication. Elliptical Curve Cryptography (ECC) and Advanced Encryption Standard (AES) are combined to provide encryption. XOR-DUAL RSA algorithm is considered for authentication and Message Digest-5 (MD5) for integrity. The results show that the proposed hybrid algorithm gives better performance in terms of computation time, the size of cipher text, and the energy consumption in WSN. It is also robust against different types of attacks in the case of image encryption.

Keywords: Advanced Encryption Standard; Cryptography; Elliptic Curve; Message Digest-5; XOR-Dual RSA

1. Introduction

Wireless sensor networks (WSNs) have a great vulnerability due to the broadcast nature and dangerous environment. Correspondingly, there are many solutions for the security issues such as routing security (Fouchal et al., 2014; Hayajneh et al., 2013; Lasla et al., 2014; Farouk et al., 2014), secure localization (Yu et al., 2013), and key management and cryptography (Mary Anita et al., 2015). Cryptographic algorithms are an essential part of the security architecture of WSNs.

WSNs suffer from many constraints such as low battery life and small memory. Due to these limitations, WSN is not able to deal with traditional cryptographic algorithms. Two main problems related to security algorithms arise in WSNs. First, the overload that security algorithms introduce in messages should be reduced at a minimum; every bit

* Corresponding author. Tel.: +20 1009067030.
E-mail addresses: r.rizk@eng.psu.edu.eg (R. Rizk), engyasminalkady@yahoo.com (Y. Alkady).
Peer review under the responsibility of Electronics Research Institute (ERI).

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jesit.2015.11.005

the sensor sends consumes energy and, consequently, reduces the life of the device. Second, the memory size which refers to size of an encrypted message and the key size should also be reduced (Faye and Myoupo, 2013).

Various cryptographic algorithms have been proposed to achieve the security requirements such as Authentication, Confidentiality, and Integrity. Authentication means preventing unauthorized parties from participating in the network. Confidentiality means keeping information secret from unauthorized parties. Integrity ensures the receiver that the received data is not altered in transit by an adversary. Data authentication can provide data integrity also.

Encryption is the process of encoding information in such a way that hackers cannot read it. There are two types of encryption techniques; symmetric and asymmetric. Symmetric cryptography, also called private-key cryptography uses only one key for encryption and decryption. Common symmetric encryption algorithms include Data Encryption Standard (***DES***) (Singh and Supriya, 2013) and Advanced Encryption Standard (***AES***) (Burr, 2003). Asymmetric key cryptography, also called public-key cryptography requires special keys to encrypt and decrypt messages. Common asymmetric encryption algorithms include ***RSA*** (Frunza and Asachi, 2007) and Elliptic Curve Cryptography (***ECC***) (Kodali and Sarma, 2013). ***ECDSA*** – Elliptic Curve Digital Signature Algorithm (Balitanas, 2009) and ***ECDH*** – Elliptic Curve Diffie Hellman (Johnson et al., 2001) are based on ***ECC***.

Both symmetric and asymmetric cryptographic techniques offer advantages and disadvantages. Symmetric encryption techniques provide cost-effective and efficient methods of securing data without compromising security however; sharing the secret key is a problem. On the other hand, asymmetric techniques solve the problem of distributing the key for encryption however; they are slow compared to symmetric encryption and consume more computer resources. Therefore, the best possible solution for encryption is the complementary use of both symmetric and asymmetric encryption techniques. Hybrid encryption attempts to exploit the advantages of both kinds of techniques while avoiding their disadvantages. Hashing creates a unique, fixed-length signature for a message or data set. It is commonly used to check data integrity. Message Digest-5 (***MD5***) (Hossain et al., 2012) algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. It has been utilized in a wide variety of security applications.

In this paper, a hybrid cryptography algorithm is proposed and presented. It is designed to provide data security and users authenticity. It includes two phases work at the same time. In Phase I, it takes the advantages of the combination of both symmetric and asymmetric cryptographic techniques using both ***AES*** and ***ECC*** algorithms. In Phase II, ***XOR-DUAL RSA*** is used since it is more robust and cannot be easily attacked. In addition, Hashing is also used for data integrity using ***MD5*** to be ensured that the original text is not being altered in the communication medium. The proposed algorithm has high operation speed, high security performance and strong usability.

The organization of this paper is as follows: Brief overviews of related works of some existing protocols are presented in Section 2. The proposed hybrid encryption algorithm is introduced in Section 3. Sections 4 and 5 present the numerical results and the simulation results of the proposed algorithm in WSNs; respectively. Section 6 presents the implementation of the proposed algorithm in the image protection application. Finally, the main conclusion is presented in Section 7.

2. Related work

To date, many cryptography algorithms have been proposed but a lot of them are not complete suitable for WSNs. In Subasree and Sakthivel (2010), a security algorithm architecture is proposed by *Subasree*. In this algorithm, the given plain text is encrypted using ***ECC*** and the derived cipher text is communicated to the destination through secured channel. Simultaneously, the Hash value is calculated through ***MD5*** for the same plain text, and then encrypted with ***DUAL RSA.*** The encrypted message of this hash value is also sent to the destination. In this algorithm, it is difficult to extract the plain text from the cipher text, because the hash value is encrypted with ***DUAL RSA*** and the plain text is encrypted with ***ECC***. The new hash value is calculated with ***MD5*** and then it is compared with decrypted hash message for its integrity. By which, it is ensured that either the original text being altered or not in the communication medium. This is the primitive feature of this algorithm however, there are two disadvantages. First, the message is encrypted by asymmetric encryption algorithms (***ECC*** and ***DUAL RSA***) that are slow compared to symmetric encryption. Second, if an attacker determines a person's private key, his or her entire messages can be read.

In *Dubal* security algorithm architecture (Dubal et al., 2011), the given plain text is encrypted with a key that is generated by ***ECDH***. The encryption algorithm used is ***DUAL RSA***. The derived cipher text is appended with the digital signature for more authentications, generated by the ***ECDSA*** algorithm. Simultaneously, the Hash value of this encrypted cipher text is taken through the ***MD5*** algorithm. Then, the generated cipher text and the signature are