Commun Nonlinear Sci Numer Simulat 17 (2012) 3267–3278

Contents lists available at SciVerse ScienceDirect

Commun Nonlinear Sci Numer Simulat

journal homepage: www.elsevier.com/locate/cnsns

Design and statistical analysis of a new chaotic block cipher for Wireless Sensor Networks

Yanbing Liu [a,b,*], Simei Tian [a], Wenping Hu [a], Congcong Xing [c]

[a] *School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
[b] *College of Computer Science and Technology, Chongqing University, Chongqing 400030, China*
[c] *Department of Mathematics and Computer Science, Nicholls State University, Thibodaux, LA 70310, USA*

ARTICLE INFO

Article history:
Received 30 June 2011
Received in revised form 2 October 2011
Accepted 22 November 2011
Available online 2 January 2012

Keywords:
Wireless Sensor Network
Chaos
Block cipher
S-box

ABSTRACT

Security issue is a vital and active topic in the research of Wireless Sensor Networks (WSN). After surveying the existing encryption algorithms for WSN briefly, we propose a new chaotic block cipher for WSN and then compare the performance of this cipher with those of RC5 and RC6 block ciphers. Simulation result demonstrates that better performance in WSN encryption algorithms can be achieved using the new cipher.

1. Introduction

It is well-known that information transmitted across Wireless Sensor Networks (WSN) can be easily intercepted by attackers due to the way WSN are constructed. Security issues of WSN have been studied as an important point in WSN research field and are getting increasing attentions. Current major researches on WSN security focus on the following areas: key management, authentication protocol, encryption algorithm, secure routing, intrusion detection, Dos attack and access control [1]. Among these areas, encryption algorithm is of great importance and has been extensively studied over the years.

Chaos is a stochastic process in nonlinear dynamic systems. Chaotic sequences can be characterized by being periodic, divergent, bounded, and sensitive to initial conditions/parameters, which allows chaos to be widely used in the research of cryptography, as evidenced by chaotic stream ciphers [2,3], chaotic block ciphers [4–6], and chaotic public key encryptions [7,8]. Among existing encryption algorithms for WSN, RC5 has known security flaws; RC6 introduces more energy consumptions due to its multiplication algorithm; AES and DES take up too much space; an integer chaotic encryption algorithm based on WSN and WSNHC has excessive energy consumptions. We, in this paper, propose a new chaotic encryption algorithm for WSN which has relatively low energy consumptions, does not require complex operations, and can achieve the security requirements of cryptographic algorithms by improving algorithmic diffusions. Note that it is difficult to directly apply a chaotic system to the WSN due to the constraints of the WSN nodes in terms of storage, processing, and computing power. Hence, a chaotic S-box algorithm based on Logistic and Baker maps is designed to obtain a balance in energy consumption, security level and memory usage. We perform some initial tests on the newly proposed algorithm and compare its behaviors with that of the popular RC5 and RC6 ciphers. The comparison results show that our new cipher outperforms RC5 and RC6 in terms of diffusion.

[*] Corresponding author at: College of Computer Science and Technology, Chongqing University, Chongqing 400030, China.
E-mail address: liuyb@cqupt.edu.cn (Y. Liu).

1007-5704/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.cnsns.2011.11.040

The rest of the paper is structured as follows. Section 2 presents an overview for the existing encryption algorithms in WSN; Section 3 describes the design of BCC; Section 4 compares the performance of BCC with that of RC5/RC6; and Section 5 concludes the paper and suggests future work.

2. Preliminaries

2.1. Overview of the RC5 and RC6 block ciphers

The popular encryption algorithms include Skipjack, RC5, RC6, Rijndael, Twofish and MISTY1. Although Rijndael meets the AES standard, it suffers from both hardware implementation difficulty and software complexity in both IEEE 802.15.4 and ZigBee network [9]. In other words, this algorithm cannot be suitable for WSN nodes. Considering that RC5 and RC6 are the only two encryption algorithms recommended by TinySec (Security for TinyOS) and SPINS among other security protocols which are widely used in WSN, we briefly review these two algorithms below.

RC5 Block Cipher: RC5 is a simple iterative algorithm proposed by Rivest in 1994. Its notable computing features are: massive data iterations, no need for large-sized tables, and no requirements for complex operations except the basic ones (e.g. addition, subtraction, XOR, and shift). Because of its simplicity, RC5 enjoys a high usability and popularity in WSN. Nevertheless, studies have shown that RC5 has diffusion problems causing certain security risks. For example, Biryukov and Kushilevitz broke RC5-32/12/16 with just 2^{44} plaintexts and RC5-32/16/16 with 2^{61} plaintexts. Miyaji broke RC5-32/10/16 with $2^{63.67}$ plaintexts at a rate of 90% [10].

RC6 Block Cipher: To resolve the security issues of RC5, RC6 was proposed. RC6 uses 4 registers and adopts the 32-bit integer multiplication as well to improve its diffusion. However, the introduction of the multiplication operation also gives rise to problems. According to [11], the energy consumption of RC6 is 7 times higher than that of RC5. Moreover, RC6 is more difficult to be implemented than RC5 in the sense that the time required for multiplications is twice as much as that of other operations for typical processors because multiplications usually require sustained energy consumption and time support, and that RC6 increases hardware costs. Therefore, the performance of RC6 is actually not as good as expected when it is used in the 32-bit processor environment where the multiplication operation is not strongly supported.

2.2. Chaotic maps

Messages encrypted using chaos sequences are difficult to be deciphered when intercepted. This is mainly due to the cryptographic properties of chaos sequences such as aperiodicity, unpredictability, and sensitivity to initial conditions and parameters. The chaotic maps used commonly include: Logistic Map, Baker Map, Lorenz Map and Super chaotic System of Cellular Neural Networks. Logistic Map and Baker Map are the computation models used in our work and are briefly explained below.

The discrete Logistic Map [12] is given by

$$x_{n+1} = \mu x_n(1 - x_n), \quad \mu \in (0,4),\ x_n \in [0,1], \tag{1}$$

where μ is the parameter of the Logistic Map. When $0 < \mu \leqslant 3$, the sequence is stable. When the value of μ increases gradually, periodic behaviors can be observed from the sequence; when $\mu > 3.5699$, periodicity disappears and chaos shows. The continuous two-dimensional Baker Map defined on the unit square [13] can be expressed as:

$$B(x,y) = \begin{cases} \left(2x, \frac{y}{2}\right), & 0 \leqslant x \leqslant \frac{1}{2}, \\ \left(2x-1, \frac{y}{2}+\frac{1}{2}\right), & \frac{1}{2} \leqslant x \leqslant 1. \end{cases} \tag{2}$$

Logistic Map and Baker Map are simple chaotic systems, so we will use these two maps to design our S-box. The detailed process will be shown later.

2.3. Related work

In this section, we present a brief survey of the related work in the area of chaotic ciphers with respect to WSN. Some block ciphers based on chaotic maps were proposed in [4–6]. Although these chaotic block ciphers work fine with their own distinguished features, they were designed without taking the specifics of the underlying networks into considerations. As a result, these chaotic block ciphers may not be able to work effectively in WSN. In fact, WSN is special in the sense that it has limited computing power and accuracy, and thus can hardly handle any floating-point operations. Considering that the sequence generated by chaotic maps consists of all floating-point numbers, it can be easily seen that using these chaotic block ciphers in the environment of WSN would be infeasible.

For the reason above, an integer chaotic block cipher based on Feistel structure was proposed in [14–16]. The basic idea is: (1) divide the plaintext into bytes which are then altered through bit permutations; (2) apply 4 rounds of Feistel encryption to the result from (1) (see below for the steps for generating the round function *f*); and (3) perform one more cycles of bit permutation to the result from (2) to finish the process.