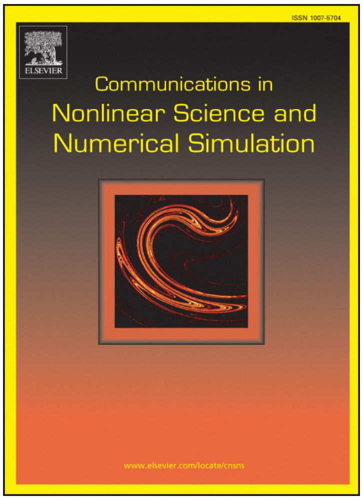

A novel compound chaotic block cipher for Wireless Sensor Networks

Xiao-Jun Tong, Zhu Wang, Yang Liu, Miao Zhang, Lianjie Xu

PII:	S1007-5704(14)00494-8
DOI:	http://dx.doi.org/10.1016/j.cnsns.2014.10.021
Reference:	CNSNS 3392
To appear in:	*Communications in Nonlinear Science and Numerical Simulation*
Received Date:	18 November 2013
Revised Date:	19 February 2014
Accepted Date:	14 October 2014

A novel compound chaotic block cipher for Wireless Sensor Networks

Xiao-Jun Tong, Zhu Wang, Yang Liu, Miao Zhang, Lianjie Xu
School of Computer Science and Technology, Harbin Institute of Technology, Weihai, 264209, China
E-mail: *tong_xiaojun@163.com*

Abstract: The nodes of wireless sensor network (WSN) have limited calculation and communication ability. Traditional encryption algorithms need large amounts of resources, so they can not be applied to the wireless sensor network. To solve this problem, this paper proposes a block cipher algorithm for wireless sensor network based on compound chaotic map. The algorithm adopts Feistel network and constructs a Cubic function including discretized chaotic map, and its key is generated by the compound chaotic sequence. Security and performance tests show that the algorithm has high security and efficiency, low resource depletion. So the novel chaotic algorithm is suitable for the wireless sensor networks.

Keywords: Chaotic map; Compound block cipher; Wireless sensor network

1 Introduction

As a new kind of technology, wireless sensor network (WSN) becomes a research hot spot. WSN consists of a large number of low-cost micro sensor nodes, which is a multiple hops self-organizing network formed by the wireless signal communication, and it is used to monitor physical or environmental conditions[1]. Sensor nodes usually work in the public occasions such as in the sea and forest, so these nodes are vulnerable[2]. WSN can be used not only in national defense but also in the field of people's livelihood such as health care[3]. The relevant information is important and sensitive. So the security of WSN is increasingly important and is getting increasing attentions.

The low computing power, limited storage resources and less energy of WSN lead to high requirements for encryption algorithm. Compared with the symmetric encryption algorithms, asymmetric encryption algorithms have higher security. But the complex operations cost more time, so the asymmetric encryption algorithms are not suitable for WSN. At present, the research on WSN encryption technology focuses mainly on the symmetric encryption algorithms.

RC5[4] and RC6[5] use mainly the operations of modular addition, shift, XOR, etc.. These operations are common on a microprocessor, so they are suitable for WSN. Compared with RC6, RC5 is more suitable for sensor network environment. But RC5 is protected by the patent. In recent years, chaos cryptology has gained many achievements. Dong BH. et al.[6-8] put chaos theory into stream cipher system, and Tenny R. et al.[9-11] proposed a public key encryption method in chaotic system. Chen S.[12] designed a chaotic block cipher based on discrete Logistic map, the encryption algorithm had fast speed and low resource consumption, but the key space was small. Moreover it can be deciphered by the differential analysis[13]. By analyzing the characteristics of the chaotic stream cipher and the chaotic block cipher, we find that the chaotic block cipher has lower consumption, so it is more suitable for WSN[14].

Based on the characteristics of WSN, combining with the chaotic technology and the block encryption structure, this paper proposes a block cipher for WSN based on discretized compound chaotic map (hereinafter referred to as: CWSN). The proposed algorithm has a comprehensive consideration between the resources and the security. **The statistic analysis, information entropy analysis, confusion and diffusion analysis, SP 800-22 tests, speed and space tests have shown that the algorithm**