Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 408 – 414

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Symmetric Key Encryption Technique: A Cellular Automata based Approach in Wireless Sensor Networks

Satyabrata Roy[a], Jyotirmoy Karjee[b], U. S. Rawat[a], Dayama Pratik N.[c], Nilanjan Dey[d]

[a,b,c]*School of Computing and IT, Manipal University Jaipur, Jaipur, Rajasthan, 303007, India*
[b]*Techno India College of Technology, Kolkata, West Bengal, 700156, India*

Abstract

Cellular Automata (CAs) is one of the most engrossing field for encrypting sensor data applied in Wireless Sensor Networks (WSN). In wireless communications, requirement of security and privacy of information is must. Therefore, transmission of sensor data over wireless communication channel plays a crucial role using cryptography techniques. The usage of cryptography characteristics of cellular automata are still not much explored in WSN. Hence in this paper, we present a symmetric key cryptography technique of block cipher using cellular automata (CAs) rules applied to sensor data in WSN. This cryptography technique uses non- complemented cellular automata rules and hybrid CA rule vector to form a group cellular automata that would be used to encrypt and decrypt sensor data. Proposed methodology has been implemented in C to validate the results.

© 2016 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of organizing committee of the ICISP2015

Keywords: Cryptography technique, cellular automata, encrption, decryption, plaintext, ciphertext, wireless sensor networks.

1. Introduction

The use of Micro-Mechanical Systems (MEMS) in wireless sensor nodes [1] plays an important role for extracting raw data in space and time. Sensor nodes extract raw data (e.g. temperature, humidity, seismic event, pressure, etc.) in Wireless Sensor Networks (WSN) from an event [2]. Thus, WSN are event based networks which collectively extract raw data in any geographical region. Once the raw data is extracted, WSN transmits it's to base station (B.S). Since the main objective of WSN to collect event features and transmit data through wireless channel, sensor nodes are much more vulnerable to attacks while transmitting data wirelessly. Hence a secure channel must be established between each sensor node and the B.S while transmitting sensor data in WSN. Thus sensor data must be encrypted before transmitting through wireless channel and decrypted at the B.S in WSN.

1877-0509 © 2016 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.082

In WSN, sensor data may have prior knowledge of signal statistics or with unknown signal statistics [3]. Prior knowledge of signal statistics means the sensor systems have the knowledge of variance and covariance of the signal extracted in the environment. This type of system modelling is quite easy to model in WSN. But modelling of signal statistics with unknown variance and covariance of signal is very complex, since sensor data is extracted at real time application in WSN. Thus secure transmission of sensor data at real time application is a challenging task as it is always needed for various confidential operations or many other private data sharing operations in WSN. Transmitting sensor data and keeping that safe from the intruders, cryptography is one of the most approached techniques in WSN. There are two types of techniques used for encryption and decryption – first is symmetric key cryptography and second is asymmetric key cryptography. Encryption may be achieved by two types of ciphering schemes – stream cipher and block cipher as mentioned in [4]. John Von Neumann [5] proposed the concept of cellular automata (CAs).

In the past two decades many area of applications of cellular automata (CAs) is being explored by many researchers as mentioned in [6]-[13]. Applications of cellular automata are used in different fields like: - Physics, Chemistry, Mathematics, Biology, Computer Science, Communication and Engineering, etc. Cellular Automata (CAs) have some specific characteristics like- randomness, correlation-immunity, nonlinearity, easy to implement, etc. These characteristics agree with the essential cryptographic properties. In this paper, a new idea is represented in which a CA based cryptosystem is generated for sensor data in WSN. This cryptosystem shows high quality of randomness of the patterns which have similar significances regarding the older computational techniques of cryptography [4] applied in WSN. Further enhancement of quality of randomness can be embedded with the help of using programmable cellular automata (PCA) [6], [7]. The suggested cryptographic technique in this paper uses a single block of 1-D PCA applied in WSN.

The paper is organized as follows. In section 2, we motivate our work using symmetric key algorithm applied in WSN where a cluster of sensor nodes transmits its encrypted raw data to the B.S. In section 3, we describe mathematical model of the proposed algorithm. We validate and conclude our work in section 4 and 5, respectively.

2. Motivation

In symmetric key cryptosystem, only one key is used for the performing encryption and decryption. This key is kept secret between sender and receiver. The sensor data has been encrypted using L2D-CASK in [14] where FPGA were used. In this paper the authors has proposed a scheme that used a key-length of 128 bits. Here in our scheme, a hybrid CA rule vector [6] has been applied on an 8-bit block that uses simple EXOR operations either on 3 bits or on 2 bits of this block. Sensor nodes are basically low computing device with less memory space. Hence our proposed scheme plays more efficient role in terms of memory and computational complexities without compromising with generated cipher text as CA has inherent chaotic sequence generation property [15]. Our scheme gives equivalent encryption efficiency as that of AES [16]. Besides, the scheme is resistant to various cryptanalysis attacks like brute force attack [14], linear cryptanalysis attack and its variants. In [17], the authors have applied Reversible Cellular Automata (RCA) based asymmetric key encryption approach using more than one byte key length whereas in our work we have used symmetric key encryption with one byte block length only at a time because of the memory limitations at sensor nodes. Since, a cluster of sensor nodes transmits its data to CH node, we use a single key at the CH node for encryption and at the B.S for decryption whereas in [17] and the key distribution is much more complex. In [18], cellular automata is used for authentication of each node in WSN.

Cellular automata is an infinite lattice of cells capable of storing one bit at a time. Each cell has the capability to transit into a new state depending on its own state and that of its neighbours [7]. Formally, a cellular automaton is defined as three tuple (S, T, N) where S is the finite and non-empty set of states, T is the finite and non-empty set of transition rules, and N is the non-empty and finite set of neighbourhood cells. The transition of each state is described under some transition rules, some examples of which are shown in Table 1.

دریافت فوری ← متن کامل مقاله

ISIArticles
مرجع مقالات تخصصی ایران

- ✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
- ✓ امکان دانلود نسخه ترجمه شده مقالات
- ✓ پذیرش سفارش ترجمه تخصصی
- ✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
- ✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
- ✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
- ✓ دانلود فوری مقاله پس از پرداخت آنلاین
- ✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات