Chapter 20
Particle Swarm Optimization-Based Session Key Generation for Wireless Communication (PSOSKG)

Arindam Sarkar
University of Kalyani, India

Jyotsna Kumar Mandal
University of Kalyani, India

ABSTRACT

In this chapter, a Particle Swarm Optimization-Based Session Key Generation for wireless communication (PSOSKG) is proposed. This cryptographic technique is solely based on the behavior of the particle swarm. Here, particle and velocity vector are formed for generation of keystream by setting up the maximum dimension of each particle and velocity vector. Each particle position and probability value is evaluated. Probability value of each particle can be determined by dividing the position of a particular particle by its length. If probability value of a particle is less than minimum probability value then a velocity is applied to move each particle into a new position. After that, the probability value of the particle at the new position is calculated. A threshold value is selected to evaluate against the velocity level of each particle. The particle having the highest velocity more than predefined threshold value is selected as a keystream for encryption.

1. INTRODUCTION

Cryptography is the practice and study of techniques for secure communication in the existence of third parties (called adversaries). More usually, it is about constructing and analyzing protocols that conquer the way of adversaries and which are associated to a variety of aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation (Feistel, 1976). Currently new computational environment becomes more distributed, more diverse and more global; the transmission

DOI: 10.4018/978-1-4666-8291-7.ch020

of information is becoming more vulnerable to adversary attacks. Now-a-days appropriate cryptographic technique in light weight devices having very low processing capabilities or limited computing power in wireless communication is the major challenge (Liddell H. G. & Scott R, 1984; Rivest R. L., 1990; Sarkar Arindam & Mandal J. K., 2013). Thus making the design of light weight cryptographic schemes for low processing devices that can counter new cryptanalysis techniques in wireless communication is becoming harder. Therefore, computer network security is a fast moving technology in the field of computer science. Network security using cryptography originally focused on mathematical and algorithmic aspects. As security techniques continue to mature, there is an emerging set of cryptographic techniques always. This advancement of digital communication technology benefitted the field of cryptography. The efficient cryptographic schemes were designed and implemented and also broken subsequently over time (Maurer U., 1993; Delgado-Restituto M., de Ahumada R.L. & Rodriguez-Vazquez A., 1995).

Swarm intelligence (R. C. Eberhart, & J. Kennedy, 1995) is aimed at collective behaviour of intelligent agents in decentralized systems. Most of the basic ideas are derived from the real swarms in the nature, which includes Particle swarm, ant colonies, bird flocking, honeybees, bacteria and microorganisms etc. Swarm models are population-based and the population is initialized with a population of potential solutions. These individuals are then manipulated (optimized) over many several iterations using several heuristics inspired from the social behaviour of insects in an effort to find the optimal solution.

In this chapter a novel particle swarm optimization based session key generation for wireless communication (PSOSKG) has been proposed. The background for Providing broad definitions and discussions of the topic and incorporate views of others presented in the section 2. The section 3 and 4 deals with the objective of the proposed technique and detail analysis of the technique respectively. PSO based Session key generation algorithm, encryption algorithm and decryption algorithm presented in section 5, 6 and 7 respectively. Detail implementation of the proposed technique discussed in the section 8. Section 9 presents the results and analysis of the proposed technique. Conclusions are drawn in section 10 and that of references at end.

2. BACKGROUND

The advances in software technology and systems will give more computational power for cryptanalyst to break the cipher (Mantin and A. Shamir., 2001; Menezes, A.J., Vanstone, S.A. & Van Oorschot, P.C., 2001; Stallings W., 2002). As new computational environment becomes more distributed, more diverse and more global, the transmission of information is becoming more vulnerable to adversary attacks. Thus making the design of cryptographic schemes that can counter new cryptanalysis techniques is becoming harder (Dourlens S., 1995; Stinson D.R., 1995). Recently soft computing approaches provide inspiration in solving problems from various fields. Now-a-days works in the application of soft computing inspired computational paradigm in cryptography become famous. The findings show that the research on applications of soft computing based approaches in cryptography is minimal as compared to other fields. Multiple disciplines have started to work together more closely for last few decades to improve the network security for reliable communication. A number of alternative cryptosystems have gained significant attention during these periods. Soft computing is the most promising one among them. Soft Computing refers to the science of reasoning, thinking and deduction that recognizes and uses the real world phenomena of grouping, memberships, and classification of various quantities under study. As such, it is an extension of natural heuristics and capable of dealing with complex systems because it does