Chapter 13
Fuzzy Logic-Based Security Evaluation of Stream Cipher

Sattar B. Sadkhan Al Maliky
University of Babylon, Iraq

Sabiha F. Jawad
Al-Mustansyria University, Iraq

ABSTRACT

The main aim of this chapter is to provide a security evaluation method based on fuzzy logic "for a pseudo-random sequences used (mainly) in stream cipher systems. The designed Fuzzy rules consider two main parameters, which are the length of the maximum period of the key sequence obtained from Linear Feedback Shift Register (LFSR) and the entropy of the result in sequences obtained from different lengths of the shift registers. The security (complexity) evaluation method is applied to the summation generator (a type of non-linear feedback shift register) in this chapter. First it is applied to its original well-known form (with one bit memory); then the evaluation method is applied to the developed summation generator (by varying the number of the delayed bits by two and by three bits). The acceptability of the results of developed evaluation method indicates a goodness of such developed approach in the security evaluation.

INTRODUCTION

Stream cipher systems have a great role in data encryption field. The security of these systems is a direct function of the complexity of the used key sequence generators. Many scientific efforts has been made to develop a complex structure of these generators that ensures the nonlinearity and complexity of the generated pseudorandom sequences. Fuzzy logic is one of the technologies that allow realistic complex models of the real world to be defined with some simple and understandable fuzzy variables and fuzzy rules. The pseudorandom sequences generators (used in stream ciphers) can be described by a fuzzy set and degree of membership to a certain parameters of the key sequence generators (Muna, 1999), (Elmer, 2012), (Marc & Lars, 2005).

Fuzzy sets are a further development of the mathematical concept of a set. Sets were first studied formally by the German mathematician Geory Cantor (1845-1918). His theory of sets met much resistance during his lifetime, but nowadays most mathematicians believe it is possible

DOI: 10.4018/978-1-4666-7456-1.ch013

to express most, if not all, of the mathematics in the language of set theory. Many researchers are considering the consequences of 'fuzzifying' set theory, and much mathematical literature is the result (Peter, 1995). The notion of fuzzy set was introduced by Lotfi Zadeh in 1965. He developed many of the methods of fuzzy logic based on this single notion. It took a couple of decades for the rationale of fuzzy sets to be understood and applied by other scientists. Fuzzy Logic, as a robust soft computing method has demonstrated its ability in many different applications. Moreover, fuzzy systems have several important features which make them suitable for many requested applications. Various methods have been suggested for automatic generation and adjustment of fuzzy rules without the aid of human experts.

The key technology of the trusted computing is the trust platform. In theory to verify if a model is trusted is an important research task. Hence there was an approach to apply the trust level evaluation method and trusted computing model based on Fuzzy logic (Li & Dan, 2010). The Fuzzy logic was applied for classifying the decision magnitude in multiple group combined interference cancelation (MGCIC) used in the intermediate stage of collusion resilient spread spectrum watermarking in M-band Wavelet using GA-Fuzzy hybridization (Sant et al, 2013). The Fuzzy logic was applied for foundation of uncertain evidence in the information system security risk assessment. The used model provided a way to define the basic belief assignment in fuzzy measure. The model offers a method of testing the evidential consistency, which reduces the uncertainty derived from the conflict of evidence (Nan & Minqiang, 2011). An approach was proposed based on using fuzzy logic and expert system for network forensics that can analyze computer crime in network environment and make digital evidences automatically. The experimental results show that the proposed system can classify most kinds of attack types (91.5% correct classification rate on average) and provided analyzable and comprehensible for forensic experts (Niandong, Shengfeng, & Tinghua, 2009). A fuzzy logic used instead of crisp value to improve the accuracy level of event detection was proposed by (Krasmira, et al, 2012). Their proposal shows that the fuzzy logic approach provides higher event detection accuracy than other well-known classification algorithms. They developed a number of techniques that help to reduce the size of the rule based by more than 70% while preserving the accuracy of event detection for fuzzy logic to deals with trust evaluation, business-interaction review and credibility adjustment. A paper of (Stefan, et al, 2007) proposes a customizable trust evaluation model based on fuzzy logic and demonstrates the integration of post interaction process like business interaction reviews and credibility adjustment. Since the design of secure routing protocol is a critical task in Ad Hoc network, the (Jing, et al., 2006) propose a fuzzy logic based security level routing protocol (FLSL). It is based on using the local multicast mechanism and security level to select the highest security level route (which is an adaptive fuzzy logic based algorithm that can adapt itself with the dynamic conditions of mobile hosts). The proposed system results in improving the security of mobile ad hoc network. The authors claim that the FSLS routing protocol is feasible to the weak security character of MANET (Mobile ad hoc Network). The evaluation of management of Urban Ecological Security (UES) has become a hotspot in concerned sciences due to the fact that the (UES) is the basis and the core of regional and National Ecological Security. (Xiao, 2011) introduced fuzzy mathematics into (UES) evaluation and established an evaluation model. An improved multilevel fuzzy evaluation algorithm based on fuzzy sets and entropy parameters is presented in the (Li, & Shen, 2006). The authors designed the multilevel fuzzy comprehensive evaluation model of P2P network security performance, and the proposed algorithm used to make an instant computation based on the proposed model. (Angel, et al, 2010) propose development of a tool which