Evaluating the Security Level of a Cryptosystem based on Chaos

Jesus D. Terrazas Gonzalez, University of Manitoba, Canada
Witold Kinsner, University of Manitoba, Canada

ABSTRACT
This paper presents tests specially-designed for a cryptosystem based on chaotic continuous cellular automata (CCA). The degree of the cryptosystem security is assessed by evaluating its (i) stationarity, (ii) spectral fractal dimension, and (iii) surrogate data. These tools are verified with known signals before applying them to test the cryptosystem. This paper introduces (i) a robust method to determine the minimum stationary window in a given time series, and (ii) a technique to conceal a chaotic attractor based on surrogate data. These new ideas are relevant because the stationarity of a signal can be determined rapidly, and the chaotic attractor concealment enhances the cryptosystem to increase its security degree.

Keywords: Cellular Automata, Continuous-Interval Cellular Automata, Cryptosystems, Data Protection, Dynamical Systems, Fractal Dimension, Image Encryption, Network Security, Stationarity

1. INTRODUCTION

Cryptographic applications are of extreme importance to protect data in various communications systems in our modern society. Cryptographic advances provide digital communications with protection of different strengths in isolated or collaborative networks. These applications range from the Data Encryption Standard (DES) developed by IBM in the ‘70s (National Bureau of Standards, 1977), also known as the turning point of modern cryptography, to some of the latest cryptographic developments in quantum cryptography (Dayball, 2012; Kurochkin, 2011) and chaos-based cryptography (Terrazas-Gonzalez & Kinsner, 2012a).

Secure cryptosystems are necessary not only for highly specialized industries or governments, but also for common computer users. Cryptosystems provide varying degrees of security. Cryptosystems designers and researchers try to obtain products with the highest security possible. However, it is important to note that canonically secure systems do not exist. A computational system could suffer threats by its mere existence. Nevertheless, cryptosystems provide the basic defense shields for data confidentiality, integrity, and availability (CIA) in insecure environments.

DOI: 10.4018/jssci.2012070105
These defenses secure data either in storage or in transit. Cryptographic protections can be expensive in terms of configuration, storage space, bandwidth, and processing time. The design of infrastructure nodes may be impacted as well (i.e., packets may take a different processing path) (Murphy et al., 2011). Nevertheless, every digital protection that we can think of requires cryptography at some point, and the benefits of having authentication, privacy, integrity, and confidentiality is worth the trade.

Vulnerabilities currently present in different parts of the world are mainly exploited through the vast known and unknown threats that are posed in the Internet on a daily basis. These vulnerabilities can affect massive networked control systems (NCS). With this in mind, it is critical that information remains secure and that it could be protected against hacking or any form of exploitation leading to its misuse in different industries (e.g., telemedicine, national defense, or search and rescue) and infrastructures (e.g., water, electrical, oil, nuclear, gas, and chemical plants) (Zhong-Hua & Guoping, 2010).

Industrial spies can access remotely confidential information or production commands from key instruments and equipment. Malicious hackers intercept, tamper, forge, and retransmit data information and production commands transmitted over networks (Zhong-Hua & Guoping, 2010). Disruption of any of the infrastructures of NCS could cause poor product quality, production loss, environmental damage, and endanger public safety and health (Zhong-Hua & Guoping, 2010).

Attackers often design malicious code capable of spreading over the Internet, and reaching target industrial facilities through proprietary protocols. An example of this is Stuxnet that was discovered in 2010 and is known as the first cyberwarfare weapon ever (Langner, 2011). Stuxnet used the supervisory control and data acquisition (SCADA) systems as a means of distribution to target Siemens controllers. It was capable of checking model numbers, configuration details, and downloading the program code from the controller by exploiting the vendor driver dynamic link library (DLL). Also, Stuxnet performed code injection exploiting an interrupt handler that the controller operating system calls automatically every 100 milliseconds. Once in the controller, Stuxnet operated as a state machine requiring no interaction with command and control servers. Its stealthy behaviour allowed it to manipulate the controller without being noticed. Stuxnet allowed legitimate code to run while the system real inputs/outputs (I/O) were isolated by a man-in-the-middle (MIM) attack. The vulnerabilities that Stuxnet exploits are unable to be patched currently because they are not caused by software or firmware defects, but through legitimate product features. It is expected that these vulnerabilities will be removed once the vendor creates a new product generation. The major vulnerability that Stuxnet exploits is that today’s controllers do not allow digital code signing (Langner, 2011). This is an area where it is mandatory to use cryptographic tools.

The main effort in this paper is to underline the importance of cryptosystems based on continuous cellular automata for computer security through research and development. It focuses in testing a modular dynamical cryptosystem based on continuous cellular automata (CCA). This cryptosystem encapsulates dynamical systems in its constituent modules (Terrazas-Gonzalez & Kinsner, 2012a). The dynamical systems used have the property of exhibiting chaos obtained through CCA. The tests performed against this cryptosystem are based on (i) stationarity and (ii) spectrum fractal dimension. The tests are verified with known signals before using them in the cryptosystem.

The aspiration of unveiling the human capacity of cognition has been present among the science community since long time ago. The efforts made to understand cognition have influenced the creation of new disciplines as cognitive informatics introduced by Wang (2002), cognitive machines by Kinsner (2007b), and cognitive dynamic systems by Haykin (2012). Cognitive informatics, as a synergic discipline, intends to provide solutions for the overlapping research
Related Content

A Fig-Based Method for Prediction Alumina Concentration
[www.igi-global.com/article/a-fig-based-method-for-prediction-alumina-concentration/88926?camid=4v1a](http://www.igi-global.com/article/a-fig-based-method-for-prediction-alumina-concentration/88926?camid=4v1a)

Generic Cabling of Intelligent Buildings Based on Ant Colony Algorithm
[www.igi-global.com/chapter/generic-cabling-intelligent-buildings-based/72790?camid=4v1a](http://www.igi-global.com/chapter/generic-cabling-intelligent-buildings-based/72790?camid=4v1a)
Search for an Optimal Solution to Vague Traffic Problems Using the PSK Method
www.igi-global.com/chapter/search-for-an-optimal-solution-to-vague-traffic-problems-using-the-psk-method/207206?camid=4v1a

Entropy Quad-Trees for High Complexity Regions Detection
Rosanne Vetro, Dan A. Simovici and Wei Ding (2011). International Journal of Software Science and Computational Intelligence (pp. 16-33).
www.igi-global.com/article/entropy-quad-trees-high-complexity/53160?camid=4v1a