Cellular Automata Applications for Renewable Energy Monitoring

P.L. Milea, M. Teodorescu, R. Muller, M. Dragulinescu, O.Oltu, G.Tiplea, G. Stefan, S.Pompilian

Abstract — The cellular automata model is a very useful tool for various artificial intelligence applications, especially those with an important statistical behaviour. The cellular automata have proven to be dynamic systems with a very vast phenomenology and in same time a extremely elegant mathematical model that allows the modeling of apparent complex real processes. The paper presents the characteristics and advantages of the cellular automata model and, also, the principles of two applications of an artificial intelligence model, the cellular automata, in the field of renewable energy resources & consumption monitoring, for development purposes of power facilities in a distributed generation area. This activity implies to wireless monitor a set of energy sensors, which can offer real time information about primary energy potential, generated and consumed power for the case of hydro, wind and solar energy distributed low-power generators. The sensors stations are periodically sending data to a data center, which stores and process it. This communication period, as well as some sensors parameters can be wireless configured from the center. To avoid measurements or configuration data to be corrupted by an intruder, we designed an encryption algorithm based on cellular automata, which comprises a dynamic key encryption generator. The received data is also processed using a cellular automata prediction algorithm, in order to obtain useful data about generated and consumed power trends. The applications with cellular automata can be hardware implemented using hardware devices or circuits which permit such a level of parallelization, like the FPGAs. For research purposes, we evaluated the reliability and performances of these applications and tested a complex implementation using a top level FPGA development board.

Keywords—Renewable Energy, Cellular Automata Applications, Artificial Intelligence, Distributed Generation, Data Encryption, Trends, Evaluation, Monitoring, FPGA.

I. INTRODUCTION

THE interest that many researchers are showing towards cellular automata (CA) arises due to the fact that these have proven to be dynamic systems with a very vast phenomenology and in same time a extremely elegant mathematical model that allows the modeling of apparent complex real processes. Until now a series of different applications of cellular automata has been developed, including scientific and industrial applications. Due to the theoretical complexity in this field, many aspects are still to be studied and formalized and many major applications can also still be developed.

In the field of renewable energy, there are many possible applications, especially in the areas where some statistical processes are involved.

In this paper we present the characteristics and some advantages of the cellular automata model, first of all theoretically, and then, focused on two applications related to renewable power generation and optimisation.

II. PRESENTATION OF THE CELLULAR AUTOMATA MODEL

A cellular automata is a computational system that comprises a theoretically infinite network of simple finite automata, that evolve synchronistic following local laws and depending on local states. Each elementary automaton has a finite (usually reduced) number of states and is connected to his immediate neighbors in the grid. Typical networks are the linear and the rectangular network, in two or more dimensions.

The state of the cellular automaton at a certain moment in time is completely defined by the states of all the cellular automata at that moment.

In the base model, all elementary automata, called cells, follow the same transition laws, the same evolution diagram. The states of the nearby cells also intervene in the transition laws. This means that the state of a certain cell at the moment t+1 depends on her own state at moment t and also on the states of the nearby cells at moment t. Thus, the global cellular automaton evolves following local states and rules.

The elementary automata have the structure of a semiautomata, because the outputs are the same as the state variables: we can see the global state of the automaton as being the “map” of the local state variables.

The evolution of the automaton states occurs through the synchronous reallocation of the local state variables. Thus the cellular automata are inherently parallel systems and are even viewed as a paradigm of parallel calculus, like the Turing machine for sequential systems.

The typical applications for cellular automata range from games theory to ecologic simulations, but the most desired goal of the researchers in this field is to deduct, based on the study of the behavior of cellular automata, the basic laws of self-organization (using the cellular automata as a mathematical model of complex natural systems).

Indeed, many complex natural systems have simple components. Their complex behavior and the self-organization seem to appear through cooperation of the parts, that follow local laws (physical, chemical, etc.). Cellular automata also have this characteristic: although composed from simple elements (that evolve following simple local rules), their
behavior is apparently complex and also shows self-organization processes (through apparition of spatial and/or temporal patterns).

For example, let's follow the evolution of a extremely simple cellular automaton. The cells, or elementary automatons are connected in a rectangular grid, as shown in Fig. 1, where the cells are represented by the squares and have two possible states: 0 (drawn as white) and 1 (drawn as black).

The next state of cell C depends on the actual states of the four neighbors: the cells N,S,V,E (named after the cardinal points) and on its own state, following a simple logical rule, that is XOR over five variables.

![Fig. 1 Fragment of a bidimensional cellular automaton](image)

![Fig. 2 The initial state of the discussed cellular automaton with the XOR law.](image)

The initial state of the automaton is presented in Fig. 2. The three pictures in Fig. 3 are three states in the evolution of this automaton. We observe the very interesting shape resulting from the initial figure.

![Fig. 3 Three states in the evolution of the cellular automaton with the initial state presented in Fig. 2](image)

The same simple local rule, XOR over five variables, produces, starting from a central point as initial state, symmetrical patterns as presented in Fig. 4, in the order of evolution.
This example can suggest the interest granted to self-organization in the case of cellular automata and also the apparent complexity in their evolution.

A. Systems’ auto-organization and the CA complexity

In the field of cellular automata, we often deal with complexity and auto-organization, these two aspects being some of the most remarkable of their characteristics. This is why we will go deeper into these notions.

Self-organization is one of the most interesting phenomena that is known. It characterizes natural complex systems and implies a globally regular behavior or the occurrence of a ordered structure, starting from random or chaotic initial states. The respective systems often comprise simple elements with laws of evolution that can be determined and thus known.

Self-organization is the manifestation of a global (macroscopic) order, based on local rules (microscopic order).

The self-organizing computing systems tend to duplicate this behavior. Generally speaking, the category of self-organizing systems comprises neural networks and cellular automata.

In the case of neural networks, self-organization manifests itself through reconfiguring the systems in order to have a certain behavior. For cellular automata, self-organization has a similar meaning to the physical phenomenon described earlier: these systems can have a global order that is determined by local evolution laws.

Cellular automata are mathematical idealizations of physical systems, in which space and time are discrete and the physical quantities can take only certain discrete values. They consist of a regular net of very simple processing elements (elementary automata), that interact locally and evolve based on local laws. Thus, cellular automata are inherently parallel.

Despite their structural simplicity, cellular automata have a very various behavior. We do not call it complex, because we cannot obtain something more complex than the network of cells itself.

Self-organization is one of notions very often used, without being rigorously defined – the same happens for the term of information. Generally speaking, we could say that self-organization is a behavioral property of complex systems, that consists of the apparition of ordered structures (spatial patterns) or an “ordered” evolution (time pattern), or even a combination of both (time-space pattern). This property is contrary to the second law of thermodynamics, that states that the entropy of a reversible closed system always increases. Yet, dissipative irreversible systems or those that interact with the environment can evolve from “disordered” states to ordered “states”.

In addition, there has been observed not only that the natural complex systems have this ability to self-organize, but also these complex systems, regardless of their nature, follow astonishing similar rules.

We can say that self-organization refers to structure and/or behavior.

In the first case, we speak of the appearance of ordered structures, like the forming of snowflakes or crystalline structures. There also exist the possibility of a periodic behavior, as for example in certain chemical reactions.

Another perspective upon the same phenomena can consider as an essential characteristic the fact that in complex systems, that comprise a lot of components, these cooperate harmoniously in order to realize certain functions or even a structure. Certain life forms offer a good example for self-organization, manifesting themselves at a functional level, like, as an example, the perfect cooperation of cells in an organism.

At a essential level, self-organization implies the apparition or manifestation of a property or a general (macroscopic structure) based on local properties.

Classical theoretic studies on self-organization involve the use of a extremely sophisticated mathematical formalism (based on Boltzmann transport differential equations), without resulting in definitive results on the matter. Cellular automaton can be considered a class of mathematical models for study of this phenomenon. They are sufficiently general to allow the simple modeling of a great variety of physical, chemical and biological systems. Especially after Stuart Kauffmann proposed the use of cellular automata to describe the differentiation of biological cells, various simulators and studies have been realized based on this model.

The very good result reported in modeling of some self-organization phenomena, like the crystal growth or the forming of snowflakes with cellular automata, support the opportunity
of their use for modeling of self-organisation. Furthermore, researchers make use of them in order to deduce the “fundamental laws” of self-organization and for establishing the “science of complexity”.

By means of their structure (a net of simple and identical elementary automata), cellular automata are alike to natural systems, that are often composed from extremely simple elements that interact only with neighboring elements, following some very simple rules. This is why cellular automata are a very good model for self-organizing systems, like energy generation-consumption systems or natural systems.

The global defining features of the cellular automata are the following:

- it is discrete in space (cellular structure)
- each cell has a finite number of states, the number of states of the automaton being thus also finite
- all the cells and thus the whole automaton evolves discretely over time
- homogeneity: all cells are identical
- the system is synchronous (and in simulations it does not matter in what order the reallocation of the states of the cells is done)
- the local rules are deterministic and following, the evolution of the whole system is deterministic (but this does not mean that is easy to foresee)
- the rules are spatially local (they depend on a number of neighbors) and temporally local (they depend on a fixed number of anterior states, usually only one)

In fact, each of this features is a simplifying hypothesis in the construction of cellular automata, that eases a lot their analysis and simulation. Although they are build out of discrete cells, systems with a very large number of components can have a practically continuous behavior.

Here we must notice the following: the limit conditions that appear due to the fact that real automata are not infinite, imply that we define different rules and/or vicinities for the cells on the edges.

B. Variants of the ideal model of CA

Real automata are first of all finite. Through their cyclic definitions (the edges of the grid are adjacent), they can be considered perfect homogenous.

Beside this automata (called standard automata), we studied an applied some variants of the model, called modifications or generalizations. They are the following:

1. Cellular automata with structured state space: due to the significance of the state, a structuring of the space of the states (considered to be the combination of state variables with precise significance) can be done. In a way, the dimension of the space of local laws decreases, making possible the study and implementation of these automata.

2. Inhomogeneous or hybrid automata, in which the topology is not uniform, this means that not all the cells have the same local laws or the local laws vary in time.

3. Multilayer automata, build from a hierarchical structure of cellular automata that interact, used especially as computational models for biological systems and more recently for the modeling of cognitive processes.

4. Asynchronous automata, in which the states of the cells are updated in a certain order. For the computation of the next state of a cell, the updated states of the neighboring cells are considered.

5. Cellular automata with memory, in which the next state of a cell depends also on a number of previous states of the same cell. From a certain point of view, these cellular automata can be considered distributed nets of elementary processors.

6. Undeterministic and probabilistic automata, very useful in modeling of real processes, in which the next state is computed undeterministic or according to a certain probabilistic distribution. These automata cannot be used for computing applications.

7. Composed automata, that comprise in their space autonomous mobile structures that interact with the cellular automata. These automata are useful in modeling of physical systems where, for example, appear different types of particles.

III. RENEWABLE ENERGY CA APPLICATIONS

The applications described in the following are related to an activity which implies to wireless monitor a set of energy sensors, which can offer real time information about primary energy potential, generated and consumed power for the case of hydro, wind and solar energy distributed low-power generators. The sensors stations are periodically sending data to a data center, which stores and process it. This communication period, as well as some sensors parameters can be wireless configured from the center. To avoid measurements or configuration data to be corrupted by an intruder, we designed a cellular automata encryption application which comprises a dynamic key encryption generator.

The second application is refering to that received data is also processed using a cellular automata prediction algorithm, in order to obtain useful data about generated and consumed power trends.

IV. THE ENCRYPTION APPLICATION

The researchers in the field of cryptography and artificial intelligence are constantly looking forward to achieve intelligent information security systems that are absolutely secure and also capable to encrypt and decrypt in real time, to assure rapid and complete protected communications [1].

Presently, a perfect secure encrypting method does not exist and this is a challenge addressed to cryptography and also another reason to elaborate new methods, algorithms and encryption systems.

In order to realize as secure as possible hardware cryptography methods, a selection from the most performant parallel computing architectures, based on distributed processing elements is necessary, of those that can be implemented in VLSI technology and also optimizing
performance/cost ratio.

A. Problem statement

The use of cellular automata in the field of cryptography is an idea that has been discussed in literature, but the solutions presented are far from exhausting the potential of this field.

The analysis of a cellular automaton architecture is done from general to particular and this is why it is somehow difficult; usually the analysis is done based on simulation, with statistical methods. It has to be mentioned that the deduction of the local rules that should generate a specific global behavior for the realization of complex systems is not yet solved theoretically. This goal is at the present moment of great interest and fully developing, the only approach presently indicated in literature being the evolutive one, based on genetic algorithms for an exploration based on auto-organizing properties.

On the other hand, a parallel computing architecture, that allows the efficient computing of an application with cellular automata, requires a specific rewriting of all the operations in order to efficiently use all the computing elements.

An n-step algorithm realized by a serial architecture will be finished in approximately n/m steps by an architecture with m processing elements. But this will require the rewriting of that algorithm in a parallel computing language (e.g. Paralaxis).

The basic disadvantage of parallel architectures is linked to the complexity of hardware. This can be diminished if processing elements are chosen that are specialized in simple operations and with an application-oriented structure, like the cellular automata. Such a computing structure is easy to design and to implement in hardware, due to uniformity and simplicity of the processing elements.

Such a system offers many facilities for implementation, due to specific cellular automata structure, characterized by massive parallelism, robustness (fault tolerance), simple structure and facilities for VLSI implementation. The basic characteristics of such a net of simple processing elements are the high processing speed (due to high degree of parallelism) and the inclination for dedicated applications (due to chosen rules).

A complex encrypting-decrypting system with interchangeable keys will function in real time on such an architecture, even if interchangeable keys of very large dimensions are used (in the order of 1024 bit). This system will imply the continuous change of the key, respecting a predefined law (through algorithm) in a huge space of possible variants. Thus, if a 1024 bit series is used, there will exist 21024 binary words and functions to sweep these binary words. It is obvious that such a system is very hard to break using stochastic methods.

B. Proposed Encryption Method

The encryption method based on cellular automaton is very simple but highly efficient. In the encryption as well as in the decryption process, exactly the same parameters of the implemented circuit are used. The difficulty in implementing

this encrypting method lies in the realization of the quasi-random sequence. Parameters, like the number of bits used to implement the cellular automaton, the number of neighbors and their position relative to the central cell, the evolution rule of the internal state of a cell are decisive in obtaining a quasi-random sequence of numbers. The number of keys grows exponentially related to each of these parameters. The encrypting process comprises two stages.

C. Encryption key generation

In this stage we wish to obtain the generation of a key with the length equal to the dimension of the message to be encrypted. Once the quasi-random sequence obtained, the second stage begins and the key will be combined with the initial message using different methods. The eventual determination of the status of the automaton at a given moment in its evolution does not help at all in discovering the states previous to that moment, because the evolution rules for every particular cell are not reversible functions [2].

D. Encryption function

The second stage in the encrypting process consists of combining the quasi-random number sequence provided by the cellular automaton with the information to be encrypted.

We must however consider the fact that in this encrypting method the same key is used for both encrypting and decrypting and this condition is the only one that governs the rule of combining the sequence of the cellular automaton with the information to be encrypted [3].

One of the simplest methods to implement this stage of the encrypting process is the bit by bit combination of the two sequences. We use the functions XOR and XNOR, which offer a very good protection to noises that affect the transmission channel. The receiving of an erroneously encrypted bit will reflect only in the corresponding bit in the decrypted message, not influencing the value of other bits. To avoid determination of the key when both the encrypted and the decrypted versions of the message are known, functions are used that realize an interdependence between a certain number of bits.

E. Encryption - decryption diagrams

The studied encrypting system uses a linear cellular automaton. The system functions as follows:

- An initial state for the cellular automaton is chosen and the execution is started.
- At every step P of the evolution, the XOR function between the current word of the message and the configuration of the cellular automaton is performed,
- The encrypted message consists of joining the words obtained as a result of the previous operation.

Please submit your manuscript electronically for review as e-mail attachments.
The decrypted message is extracted from the sequence of the new words obtained from the previous operation.

The method is based upon the properties of the XOR function:

\[(a \oplus b) \oplus a = a \oplus b \oplus a = b \oplus (a \oplus a) = b \oplus 0 = b.\]

The method proposed for implementation offers the possibility to extend to a set of rules, neighborhoods and limit conditions, the system being thus usable in many variants.

The encrypting and decrypting systems (presented above) are identically structured, which is a significant advantage of this method, because it requires the designing of a single circuit for implementation.

The synchronization (Start) and presetting (R) blocks were introduced in order to modify the rule used and to define the neighborhoods and the limit conditions from a fixed set.

The cellular automaton used has the following characteristics:
- Linear cellular automaton with 32 cells;
- III-rd class local rules, set of 4 local rules;
- Dimensions of neighborhood: 3, 4, 5, 6, 7;
- Optional limit conditions: cyclic or fixed edges (0 or 1).

Observations:
1. Because the cellular automaton is dimensioned for a maximum neighborhood radius of 3, the introducing of asymmetrical supplementary neighborhoods for the neighborhood dimensions of 3, 4 and 5, is possible.
2. For the maximum dimension of neighborhood (7) a single local rule will be implemented in order not to load the hardware structure with a complex combinational circuit.
3. Any neighborhood can be combined with any rule from the same set and any limit conditions.

Table 1 presents the implemented limit conditions.

<table>
<thead>
<tr>
<th>Neighborhood code</th>
<th>Cyclic connection</th>
<th>Binary connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>yes</td>
<td>4</td>
</tr>
<tr>
<td>32</td>
<td>yes</td>
<td>4</td>
</tr>
<tr>
<td>33</td>
<td>yes</td>
<td>4</td>
</tr>
<tr>
<td>41</td>
<td>yes</td>
<td>8</td>
</tr>
<tr>
<td>42</td>
<td>yes</td>
<td>8</td>
</tr>
<tr>
<td>43</td>
<td>Partial</td>
<td>8</td>
</tr>
<tr>
<td>44</td>
<td>Partial</td>
<td>8</td>
</tr>
<tr>
<td>51</td>
<td>Partial</td>
<td>16</td>
</tr>
<tr>
<td>52</td>
<td>Partial</td>
<td>16</td>
</tr>
<tr>
<td>53</td>
<td>Partial</td>
<td>16</td>
</tr>
<tr>
<td>61</td>
<td>-</td>
<td>16</td>
</tr>
<tr>
<td>62</td>
<td>-</td>
<td>16</td>
</tr>
<tr>
<td>7x</td>
<td>-</td>
<td>16</td>
</tr>
</tbody>
</table>

Observations:
- For the neighborhood radius of 3, the cyclic connection will not be fully implemented
- For the neighborhood radius of 6 and 7 the 32 respectively 64 binary combinations will not be implemented, in order to maintain a 4-bit encryption.

F. Performance Estimation

The performance estimation of cryptographic systems based on cellular automata is done in the same way as for every cryptographic system, considering the following items:
- The cost of the system;
- The time required for encrypting and decrypting...
operations;
• The dimension of the key;
• The ratio between the “dimension” of coded data and the initial “dimension”;
• Reliability regarding different types of attack;
Thus, in the particular case of cellular automata we ascertain:
• The reduced price of the physical system implemented with cellular automata;
• Reduced computing time (massive parallel system) and principally equal time for encrypting and decrypting methods selected in this paper;
• Reduced dimension of the key;
• Maintenance of the dimensions of data after encrypting;
• The resistance to attacks depends on the effective complexity and on the apparent complexity of the chosen cellular automaton.

As a very interesting fact, we observe that the encrypting application and the quasi-random sequence generation application are strongly correlated. In many situations, a good quasi-random sequence generator can be successfully used in generating the sequence needed for encrypting or for direct altering of the message to be coded.

The most “suitable” cellular automaton for cryptography are the ones in class III, the same as for quasi-random sequence generators. Usually uni-dimensional automata are used, although more “clumsy” solutions with bi-dimensional automata do exist – in this case the difficulty is given partially by the bi-dimensional transposition of the message to be coded. Generally speaking, the encrypting schemes are remarkably simple and particularly simpler than the complexity involved by decrypting of messages.

V. THE DISTRIBUTED GENERATION ENERGETIC SYSTEM PREDICTION AND MODELING

This is the second application we study to statistically predict the evolution of the consumption/generation ratio for a given area. For this estimation we know that the edge consumers can migrate easily from one generator to another, but this is not the same case for a consumer which is located in the neighbourhood of a power generator.

For this reason, in our application, we model the generated power as a flux of cellular automata population, which is searching for available consumer position, on the map. Every unit (W) of generated power is modelled as a cellular automaton, since the consumed power is represented as a resource on the local map.

A. The input data

Primary generation data are collected from the real area using a set of sensors which make measurements on the local energy resources parameters, like solar irradiance, wind speed, water flow etc., to estimate the generated power on the base of installed power. Consumption data is collected by power meters located in the nodes of the energy network.

Based on these data, the generated power is represented inside of the model as a variable CA population, while the consumed power is represented as a quasi-constant (statistical) start resources.

B. Results Interpretation

In this way, the model can optimally direct the generated power to the closer consumers (in the neighbourhood area) and the exceeding power is transported, as cellular automata migration, to other consumers areas (resources).

When the simulator is running, the main part of CA population is going to occupy closer consumer resources, other part is searching for available remote positions, and other part is dying.

In this analogy, the system is considered well designed and optimized, when the resources positions are occupied/consumed in the shortest possible time.

The population migration to remote positions is an energy transportation measure, and an inversely measure of the distributed generation systems optimization.

The dying CA population is a measure of the available/generated but not consumed energy.

In this model, the time delay to the resources occupation is a measure of distance transported power, and then, a measure of the transportation loses.

C. The Model Use

The presented CA model allow us to evaluate the current optimization of a distributed power generation system, and to take the measures to optimize it, by installing new generators or new transportation lines.

The model help us, also, to predict the energy economy and cost efficiency which will result as a consequence of the mentioned actions.

VI. HARDWARE TESTS

Throughout the research done, evaluation of the methods and testing of their implementation was chosen to be done in reconfigurable FPGA architectures.

FPGA circuits allow the implementation of a very big number of simple structures, like cellular automata, that will function independently, thus producing the effect of parallel computing with a very big number of computing elements.

These distributed processing elements will decisively influence the processing speed and is expected to have a high efficiency in cryptography applications if specific and also implementation problems are solved.

Although the purpose of his paper didn’t comprise the hardware implementation of the method, we mention that this implementation is possible, as stated in other papers [5].

We realized a new implementation using an advanced platform (RPS-3000) for ASIC/SOC logic emulation and prototyping, based on a latest generation Xilinx FPGA.
proposed, and its advantages was presented and argued.

An encrypting and decrypting application based on cellular automata with 32 cells and 4 local rules of the III\textsuperscript{rd} class was proposed, and its advantages was presented and argued. Cellular automata was proven to be an interesting option for practical realization of cryptographic systems, because they are dynamic systems with a often complex evolution, although based on simple rules, allow very performant hardware realization and permit the generation of quasi-random sequences due to their very good statistical properties.

A monitoring application was proposed to evaluate and statistically predict the evolution of the optimization of the distributed generation power system of renewable energy. The application allow us to determine some important energy indicators, very useful for urgent optimization actions, as well as for sustainable development planning.

The described and theoretically evaluated application was tested in a pre-VLSI hardware implementation. The prototype implementation confirmed the previous evaluations, proofing to be efficient and having good security invulnerability. For this reason, we concluded that the VLSI implementation will provide a cheap device with robust, versatile and efficient encryption - decryption functions which will make it suitable for portable devices (like mobile phones) integration.

ACKNOWLEDGMENT

The work reported in this paper was made within the SINERG project (PNCDI2-22-140/2008), funded by The Executive Unit for Higher Education, Research, Development and Innovation Funding (UEFISCDI).

REFERENCES


Petra Lucian Milea is scientific researcher at Politehnica University of Bucharest, Romania. He obtained a Ph.D degree in Electronics and Telecommunications Engineering at Politehnica University of Bucharest, Romania, in 2010. His main field of study is focused on monitoring and control systems for various applications, including renewable energy.

He started his work in scientific research in 1995, at the Electronics Research Institute in Bucharest, Romania, in the field of medical electronics. From 1997 he started to work at the Electronics Technology and Reliability Department of Politehnica University of Bucharest, Romania. Meanwhile he also worked, for two years, at The National Institute for Research and Development in Microtechnologies, in the field of PV cells. His current job is at Politehnica University of Bucharest, Electronics, Telecommunications and Information Technology Faculty, Electronics Technology and Reliability Department, Bucharest, Romania, Juliu Maniu Blvd. 1-3. He is also the Manager of Solaris Consult S.R.L. Bucharest – an IT consultancy and research company. His current and previous research interests include control systems, renewable energy, medical electronics, artificial intelligence, information technology.