REAL TIME MODELING AND SIMULATION ALGORITHMS FOR OPTIMIZATION OF COMPUTER NETWORKS DATA TRAFFIC

Romuald Kotowski, Beata Rubin, Grzegorz Rubin, Aneta Wiktorzak

Institute of Computer Science and Automation
Lomza State University of Applied Sciences, Lomza, Poland

E-mail: awiktorzak@pwsip.edu.pl

Abstract: An innovative approach for modeling and simulation algorithms to optimize data traffic in computer networks is presented. The proposed methodology for finding solutions, such as plug-in devices between the parties of communication, which allow for secure and compressed data transfer is briefly described. This paper shows the perspective of the research needed to find appropriate algorithms, including artificial intelligence and neural networks, and then the necessity to develop model and simulate processor architecture of the mentioned properties in real time. The approach is based on modeling using modification of Petri nets called Hardware Petri Nets implemented in form of CAD software. The hardware implementation will be on specific universal balanced architecture on Field-Programmable Gate Array (FPGA).

Key words: AI, Petri nets, FPGA, modeling and simulation, compression, encryption, real time data transmission

Introduction

The aims and objectives of this research using computer networks have become ubiquitous – without this method of communication and data exchange one can not imagine one's life or work. Data transmission technologies allowing the increase of communication speed are intensively developing all the time.

Two very important elements in data exchange are confidentiality and credibility, which ensure that the data comes from a proper and trusted source. These aspects of data transmission are important not just for individual users of computer networks, but also enterprises, particularly those with branch offices located in different places, financial institutions (banks), government offices and all other organizations. Electronic transactions have to be free from phishing and manipulation of data content. There are many methods of encryption and compilation of secure connections, but they have complicated configurations and are very expensive. Our main research goal is a technical analysis of computer networks traffic optimization for data encryption and compression. The selection and development of solutions, less expensive than currently available on the market, as well as simpler in configuration, will be done. The current methods of encrypting data traffic are offered by companies in the form of complex solutions and dedicated devices. The implementations of such solutions require trained personnel and a significant investment of financial resources. Proposed solutions in the form of a module that plugs into the network of both the sender and the recipient's cabling sides, which would satisfy the task of encryption and compression in real time, and would greatly simplify the compilation of secure connections of two distant points in the network. By choosing the appropriate algorithms, including methods and techniques of artificial intelligence (AI), it is possible to create a model and to simulate the processor architecture implementing the process of encryption and data compression sent over the network in real time. The developed solutions, having verified established operating parameters, can be used in other physical project implementations of network compression and encryption modules.

Objectives of Proposed Research and Solutions

The first research task should be focused on examining the possibility of using genetic algorithms (GA) for optimum choice of methods and algorithms to encrypt and compress data sent via computer networks. Cryptography is a basic tool for protecting and securing data. Security provides safety, reliability and accuracy. GA is typically used in order to obtain solutions for optimization and search for problems. In cryptography the selection of the public key is a selection process in which keys can be categorized on the basis of their fitness function, making GA a fine candidate for the key generation. A new approach for the e-security applications using the concept of genetic algorithms with pseudo random sequence to encrypt and decrypt data stream is proposed. Encryption and decryption algorithms try to convert data to other secured data in real time. Many different data encryption and decryption methods have been defined to keep the security of these data.

Genetic algorithm is a special kind of stochastic search algorithm that depicts the biological evolution as the problem solving technique. GA works on the search space called population [1]. Each element of the population is called as chromosome. GA begins with randomly selecting a set of feasible solutions from the population. Each chromosome is a solution by itself and is evaluated for fitness. This fitness defines the quality of a solution. GA uses an adaptive heuristic search technique which finds the set of best solutions from the population. New off springs are generated/evolved from the chromosomes using operators like selection, crossover and mutation. Most of the fit chromosomes are moved to the next generation and the weaker candidates get less chance for such relocation. This is because GA is based on the principle of Darwin theory of evolution, which emphasizes that the 'survival of the fittest'. This process repeats until the chromosomes have the best solution to the given problem [2]. Finally, the average fitness of the population increases at each iteration, so by repeating the process many times, better results are discovered. GA has been widely studied and experimented on in many fields of engineering as well as for nonlinear programming like traveling salesman problems, minimum spanning tree, scheduling problems and many others.

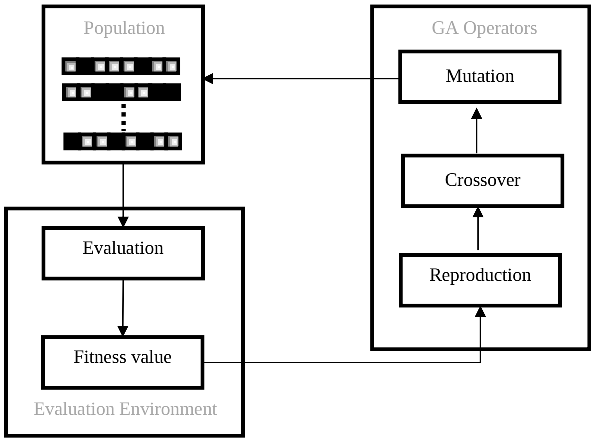

Fig. 1: Genetic Algorithm Evaluation Flow

Because the genetic algorithm technique follows from the principle of natural evolution (see Fig. 1) the idea of natural evolution is used in the proposed algorithm: first guessing the all possible solutions and next combining the most appropriate solutions to create a new generation of solution which will be better than the previous generation and will give a better fitness value.

Several solutions have been proposed in this area. For the first time in 1993 in the papers by Spillman [3,4] a genetic algorithm based approach for the cryptanalysis of a substitution cipher and another for the cryptanalysis of a knapsack cipher was presented. In these papers the possibility of random type search to discover the key (or key space) for a simple substitution cipher was explored. In the same year Mathew [5] used an order based genetic algorithm for cryptanalysis of a transposition cipher. Kumar [6] described an encryption method with the use of crossover operator and pseudo-random sequence generator by NLFSR[1] method. A pseudo-random sequence gives the crossover point, and, hence, a fully encrypted data is achieved. Kumar and Raj [6] have extended the idea further and have used the mutation after the encryption.

Garg [7] indicated that the efficiency of a genetic algorithm attack on the knapsack cipher can be improved with variation of initial entry parameters. Nalini [8] compared the attack of SDES[2] using optimization heuristics technique and GA based techniques. The results showed that GA based approach minimizes the time complexity. In the other paper Garg [9] explored the use of memetic algorithm as an extension of the traditional genetic algorithm to break a simplified data encryption standard algorithm.

Singh et al. [10] provides a new method of security that is the e-security with the help of GA and pseudo-random sequence, just to encrypt and decrypt the data.

The speed of the algorithm is good at the time of encryption process as well as safe and reliable because of the lack of knowledge about pseudo-random sequence and mutation string. Sindhuja et al. [11] gave a symmetric key crypto-system with the help of GA. Firstly, plain text is converted in the form of a matrix that is a key matrix and a text matrix; secondly, an additive matrix is produced by adding both the text and key matrices.

Analysis and testing the possibilities of the mentioned algorithms of implementation (next task) in programmable circuits will be done using Petri nets [12–14].

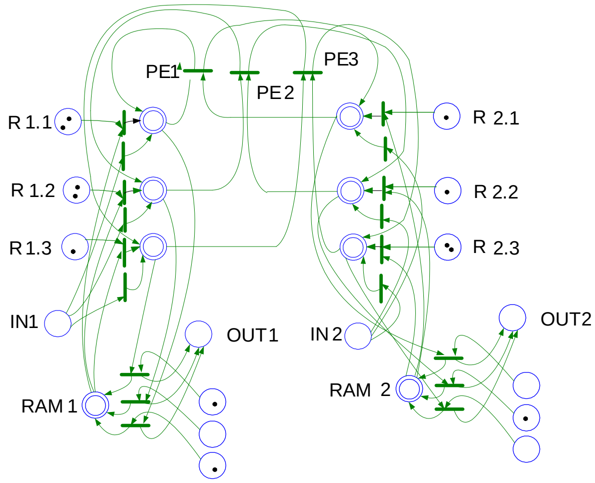

Fig. 2: Petri Nets Model of System of Balanced Bit-serial Shared Memory Universal Architecture

Figure 2 shows a Petri net model of universal computational architecture given in Figure 3. Usually, modeling

[1] NLFSR – Nonlinear Feed Forward Shift Register
[2] SDES – Session Description Protocol Security Descriptions

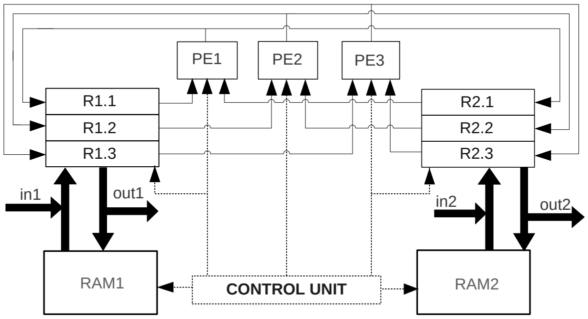

Fig. 3: System of Balanced Bit-serial Shared Memory Architecture (based on [15])

the real digital systems is done in hardware description language (HDL) [16]. Utilizing an HDL project it is possible to use one of many groups from different manufacturers of chips to design and implement systems in a programmable FPGA devices. Designed in this way the programmable systems require appropriate performance testing. Unfortunately, the preparation of appropriate error free vectors of testing is time consuming and in the case of parallel systems is often not possible. Therefore, the use of tools in preparation of test vectors appear to be appropriate, i.e. based on the Petri nets theory.

Exploring the possibility of mapping and validating algorithms on reconfigurable processor architecture implemented in programmable circuits can be done by formal methods or simulation applying graphical tools. During simulation every event which occurs step by step will be placed in a time graph. Every fired transition corresponds to the high logical level (digital one) and no fire, low logical level (digital zero).

In Fig. 4 the scheme of simulation based on the Petri nets theory step by step the behavior of the modeled system is showed. Tracking the simulation process it is possible to check in which moment the given tasks are running and there are no problems with their action. A displayed time graph corresponds to control vectors of developed system architecture. Such data can be easily applied to simulation process using tools for simulation programmable devices e.g. ISE WebPack [17] or ModelSim. That allows for verification of compliance with the requirements of the solutions working in real time.

Suchacka [18] studied the specific Web traffic in the Web server systems of the business-to-consumer sites. It was observed that the traffic is highly variable and explosive.

The other interesting approach of the modeling of the computer network traffic, and confirming the results of Suchacka, is based on the observation that the data traffic has a self-similar character [19]. It was found that the thickening and thinning of traffic in the course of events does not depend on the time scale (like seconds, minutes and hours) [20]. To measure the self-similarity of the processes the Hurst coefficient H was used

$$H = 1 - \frac{\beta}{2}\,,$$

where β is the measure of the vanishing variance of the distances between packet streams with respect to the graduated time. The proposed simulator using the Markov Modulated Poisson Process together with the Long Range Dependencies algorithm by Salvador and Valadas [21] yields very good results as compared with real data.

One of the most important goals of the modeling and simulation of the computer network traffic is the forecasting of the intensity of traffic. An interesting approach based on the econometric models is presented in [22].

Methodology and Required Tasks and Objectives of the Research

According to the goals of the proposed research, the tasks and objectives to fulfill are given below:

Task 1: Research on the theoretical and numerical optimization methods of traffic on computer networks, taking into account encrypting and compressing the data in real time. The study will be developed using theoretical mathematical models and numerical algorithms compressing and decompressing the data and algorithm to encrypt and decrypt the data. There will be also a study on expanding the theoretical basis and the interpretation of the optimization of experimental data compression, and encryption of data using genetic algorithms and artificial neural networks. The theoretical and numerical modeling and simulation of the processor architecture performing compression algorithm and encrypting data on computer networks in real time will be developed. For this purpose, they shall be deposited with research tools: encryption theory, methods, and data compression methodology, genetic algorithms, artificial neural networks, cellular automata algorithms, numerical simulations of dynamic process simulation, modeling algorithms as a function of the properties of network structures.

Task 2: The use of computer techniques to optimize traffic over computer networks taking into account the encryption and compression of data in real time. The development of numerical methods for modeling and simulation of the processor architecture performing compression algorithm and encrypting data on computer networks in real time. The development of a computer technician algorithm for compressing and decompressing data, the algorithm encryption and decryption of data compression process optimization

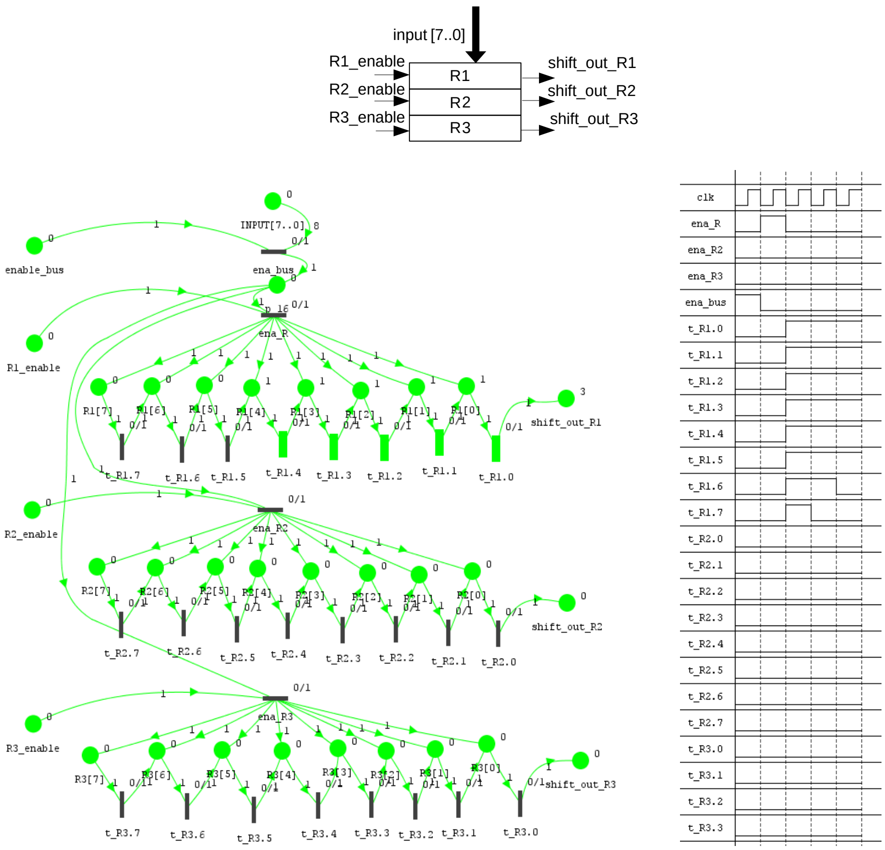

Fig. 4: Simulation of Five Steps of Three 8-bit Shift Registers Block Modeled by Petri Nets

methods and data encryption using methods and artificial intelligence techniques.

Task 3: Studies on the use of modern methods of computational intelligence in modeling processor architecture performing compression algorithm and encrypting data on computer networks in real time. This concerns mainly the use of genetic algorithms, artificial neural networks and cellular algorithms.

Task 4: The application of experimental methods: identification of a data packet transport characteristics and properties of encryption algorithms, data compression, data traffic, optimization of real-time modeling and simulation data traffic network.

Scheduled tasks will be largely based on past experience and our knowledge related to the theme of the project. In particular in the area of computer networks, programmable systems, optimization methods and techniques of artificial intelligence, modeling and simulation of processes, information, and statistics.

The Work Packages of Planned Research

To achieve presented goals stated in the paper, the following work packages should be done:

WP1: An examination of knowledge of encryption and data compression in computer networks in real-time.

WP2: An analysis of algorithms which compress and decompress data transmitted in real-time across computer networks.

WP3: An analysis of optimization of data traffic on the network using the methods and artificial intelligence techniques.

WP4: An analysis of algorithms to encrypt and decrypt transmitted data in real time across computer networks.

WP5: An application of optimization methods of compression and encryption of network traffic in real-time using genetic algorithms, algorithms phones, and artificial neural networks.

WP6: Modeling and simulation processor architecture performing compression algorithm and encrypting data on computer networks in real time.

WP7: Verification, checking and testing of optimal solutions for streaming data network.

WP8: A study of the possibility of mapping algorithms on reconfigurable processor architecture implemented in the programmable circuits.

Summary and Future Work

The planned result of scientific research will be to develop practical solutions, and select and implement the appropriate algorithms for compression and data encryption implemented in real-time reconfigurable processor architecture.

The result is a practical model of the processor architecture of network module which plugs into the structured cabling infrastructure in two distant points whose purpose is encryption and data compression. This will allow a simpler and cheaper way to set up connections encrypted data compression.

Literature

[1] E.D. Goldberg. *Genetic Algorithms in Search, Optimization and Machine Learning.* Addison-Wesley Longman Publishing Co. Inc., Boston, USA, 1989.

[2] D. Laurence. *Handbook of Genetic Algorithms.* International Thomson Computer Press, 1991.

[3] R. Spillman, M. Janssen, B. Nelson and N. Kepner. Use of genetic algorithm in cryptanalysis of simple substitution cipher. *Cryptologic*, 17 (4):1367–377, 1993.

[4] R. Spillman. Cryptanalysis of knapsack ciphers using genetic algorithms. *Cryptologic*, 18 (4):102–115, 1994.

[5] R. Methew. The use of genetic algorithms in cryptanalysis. *Cryptologic*, 17 (4):187–201, 1993.

[6] A. Kumar and N. Raj. Application of genetic algorithm in the field of steganography. *International Journal of Information Technology*, 2 (1):12–15, 2004.

[7] P. Garg. Genetic algorithm attack on simplified data encryption standard algorithm. *International Journal Research in Computing Science*, 23:115–129, 2006.

[8] N. Nalini. Cryptanalysis of simplified data encryption standard via optimization heuristics. *International Journal of Computer Sciences and Network Security*, 6 (1B):45–60, 2006.

[9] P. Garg. Memetic algorithm attack on simplified data encryption standard algorithm. In *International Conference on Data Management*, pages 1097–1108, February 2008.

[10] P. Singh, G. Gosawi and S. Dubey. GA: a technique for cryptography real time data transmission. *Binary Journal of Data Mining and Networking*, 4:37–40, 2014.

[11] K. Sindhuja and P. Devi. A symmetric key encryption technique using GA. *International Journal of Computer Sciences and Information Technology*, 5 (1):414–416, 2014.

[12] G. Rubin and K. Bielawski. Efficient simulation method for parallel digital systems control units development. In *Information Systems Architecture and Technology: System Analysis Approach to the Design, Control and Decision Support*, pages 207–216. Oficyna Wydawnicza Politechniki Wrocławskiej, 2012.

[13] G. Rubin, K. Bielawski and J. Baszun. A hardware conceptual prototyping of the genetic algorithm to adaptive iir filtering. In *IEEE Computer Society, International Symposium on Parallel Computing in Electrical Engineering: PARELEC'2006*, pages 392–395, Los Alamitos 2006.

[14] G. Rubin, M. Omieljanowicz and A. Petrovsky. Rapid prototyping of dedicated systems based on shared memory architecture: Method and example. *Zeszyty Naukowe Politechniki Białostockiej, Informatyka*, 9:105–118, 2012.

[15] L. Wanhammar. *DSP Integrated Circuits.* Academic Press, USA, 1999.

[16] G. Rubin, M. Omieljanowicz and A. Petrovsky. Reconfigurable fpga–based hardware accelerator for embedded dsp. In *MIXDES'2007, Ciechocinek*, pages 147–151, 2007.

[17] Xilinx documentation: http://www.xilinx.com.

[18] G. Suchacka. Web traffic modelling to evaluate efficiency of a bussines Web server system. *Pomiary Automatyka Robotyka*, 12:57–60, 2010.

[19] R. Wójcicki. New method of selfsimilar traffic modellingin networks based on the Poisson processes with Markov modulation. *Studia Informatica*, 26 (2):23–39, 2005. (in Polish).

[20] T. Czachórski and J. Domańska. Self-similarity of computer network traffic. *Studia Informatica*, 1 (43):93–108, 2001.

[21] P. Salvador and R. Valadas. Multiscale fitting procedure using Markov modulated Poisson processes. *Telecommunication Systems*, 23 (1,2):123–148, 2003.

[22] A. Szmit and M. Szmit. About usage of econometric models in network traffic prediction. *Zeszyty Naukowe Politechniki Łódzkiej*, 1154:193–201, 2013.