International Journal of Research in Advent Technology (IJRAT) (E-ISSN: 2321-9637)
Special Issue
National Conference "CONVERGENCE 2016", 06th-07th April 2016

Implementation of Network Security Using Genetic Algorithm

Ms. B. D. Nagpure [1], Ms. A. D. Dhote[2], Ms. P. S.Rokade[3], Ms. P. B. Kale[4], Ms. N. S .Kinhikar[5]
Computer Science And Engineering
nagpurebhagyshri@gmail.com[1], nidhiskinhikar@gmail.com[2]

ABSTRACT : Over the last few years, Secured transmission of data has been a major issue in data communication. Network security consists of the provisions and policies to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network- accessible resources.. Implement security of confidential information and data transmission using cryptography with Genetic Algorithm in order to provide confidentiality, authentication, integrity and non-repudiation of the messages. An algorithm is developed and implemented to generate a key pair. A plain text is encrypted using the Private Key of receiver to produce an intermediate cipher. The intermediate cipher is again encrypted using genetic algorithm to produce final cipher.

Keyword: Genetic Algorithm, Cryptography

1.Introduction

The application of a genetic algorithm (GA) to the field of cryptanalysis is rather peerless. This non-traditional application is investigated to determine the profit of applying a GA to a cryptanalytic problem if any. If the GA-based approach proves successful, it could lead to more faster, more automated cryptanalysis techniques. How-ever, since this area is so different from the application areas where GAs developed, the GA-based methods will likely prove to be less successful than the traditional methods. The primary goals of this work are to produce a performance comparison between traditional cryptanalysis methods and genetic algorithm based methods, and to determine the validity of typical GA-based methods in the field of cryptanalysis. A thorough search of the available literature found GA-based assault on only these ciphers. In many cases, these ciphers are some of the simplest possible version GAs attempt to solve problems through modelling a simplified private key [12]. Genetic algorithms (GAs) are a class of reduce of genetic processes.. Both traditional crypt-analysis and he results are then com-pared using the metrics of elapsed time and percentage of successful decryptions [12]Genetic algorithms are based on the mechanics of natural selection and genetics[10]..Genetic algorithm belongs to the family of evolutionary algorithms, along with genetic programming, evolution strategies, and evolutionary programming[12].

2.PROBLEM STATEMENT

Encryption method follows as: A pair of key (Public and Private) generated. In symmetric-key cryptography, it is obvious that when a text is encrypted with a private key, it is decrypted with corresponding private key and vice-versa. The plain text is encrypted using private key to produce Intermediate cipher.[1] The Intermediate cipher is further encrypted using Genetic Algorithm to produce the final cipher. Decryption method: The Final cipher is decrypted using Genetic Algorithm to get intermediate cipher which is again decrypted using corresponding private key to get the plain text.

Initial Encryption: Intermediate cipher = Encrypt (plaintext, public Key) OR Intermediate cipher = Encrypt (plaintext, Private Key)

Genetic Encryption:

Final cipher = Encrypt (Intermediate cipher**)**

Genetic Decryption:

Intermediate cipher = decrypt (Final cipher) Final Decryption= Plaintext = decrypt (Intermediate cipher, Private Key) OR Plaintext = decrypt (Intermediate cipher, Public Key)[1]

3.Genetic Algorithm

The Genetic Algorithms (GAs) are exploration algorithms based on the theory of natural selection with an inventive finesse of nature. The central idea of research on GAs has been snappy.. The implications of snappy are the removal of costly resigns and higher level of variation.

The description of a natural population is done using, what is called chromosomes. its nothing but a set of numbers, generally in binary. Each number represents a cell and can be perceived as an positive or negative answer. The initial population can be generated using any Pseudo Random Number Generator. Each chromosome is then assigned a fitness value. Based on this fitness value replication is done. Now generate a random number % 100. Now aggregative Frequency 63 lies in Chromosome some chromosome say x. Therefore, Chromosome x is replicated. The above population is enhanced by using basic operations like crossover and mutation. [4]

3.1 Population Size:

The process of a GA usually begins with a randomly selected population of chromosomes. These chromosomes are representations of the problem to be solved. According to the attributes of the problem, different positions of each chromosome are encoded as bits, characters, or numbers. These positions are sometimes referred to as **genes** and are changed randomly within a range during evolution. The set of chromosomes during a stage of evolution are called a population. An evaluation function is used to calculate the ―goodness‖ of each chromosome. During evaluation, two basic operators, crossover and mutation, are used to simulate the natural reproduction and mutation of species. The selection of chromosomes for survival and combination is biased towards the fittest chromosomes[14]. The population size remains constant from generation to generation. Determining the size of the population is a crucial factor. When the population size too small then increases the risk of converging prematurely to local minima. Initial Population can be determined by randomly or using some heuristic. The selected parents are used to generate the individuals for next generation through the application of crossover operator. For binary string individuals, one-point ring crossover, two-point, and uniform crossover are often used[12]. The Two parents are combined in the form of ring and a random cut point is generated. With reference to this cutting point, one of the children is created in the clockwise direction, while the other one is created in anti-clockwise direction, . Every position of the child must retain a value found in the corresponding position of a parent, and the child must be a valid permutation. After Crossover, threshold check is performed

3.2 Selection

It is vicenary criterion based on fitness value to select which chromosomes from population will go to regenerate. Intuitively the chromosome with more fitness value will be considered better and in order to implement commensurate random choice. Selection is an important function in genetic algorithms (GAs), based on an evaluation criterion that returns a measurement of worth for any chromosome in the context of the problem. It is the stage of genetic algorithm in which individual genomes are chosen from the string of chromosomes. The commonly used techniques for selection of chromosomes are Roulette wheel, rank selection and steady state selection [13].

3.3Crossover and mutation

Crossover is an important genetic operator that combines the two parent chromosomes to produce two new offspring chromosomes. The idea behind crossover is that the new chromosome may be better than both of the parents if it takes the best characteristics from each of the parents. Crossover occurs during evolution according to a user-defined crossover probability. In the presented approach, one point crossover technique is used. The lengths of both the parent chromosomes are checked and the chromosome whose length is smaller is taken as parent 1. If lengths of both the chromosomes are the same, then any one chromosome is taken as parent 1. Then, a crossover point is randomly chosen for parent 1.the part of both the parent chromosomes after the crossover point is interchanged Mutation occurs on only a few individuals. Each gene in each chromosome is checked for possible mutation by generating a random number between zero and one. If this number is less than or equal to the given mutation probability, i.e., 0.01, then the gene value is changed. Mutations create diversity to search in domain regions that may otherwise be excluded[10].

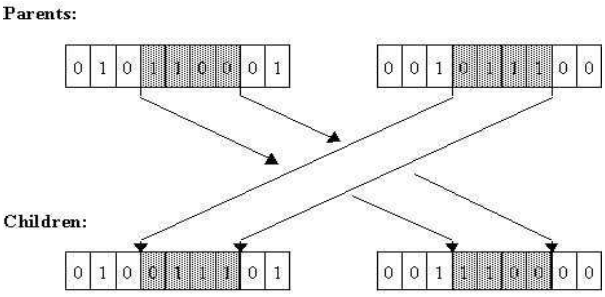

Fig 1 Crossover

3.4FITNESS FUNCTION

There are many parameters that can influence the effectiveness of the genetic algorithm. The evaluation function is one of the most important and difficult parameters in genetic algorithms. First we define a formula to calculate whether a field of the connection matches the pre-classified data set. In a chromosome header fields are taken. The data type can be character, integer, double or an object. If a particular packet has been matched to a number of rules decided and we are calculating difference zero or one, then best delta value can be computed. The Genetic Algorithms cycle is illustrated in this example for maximizing a function **f(x) = x2** in the interval **0 <x <31**[p].In our case gene means property that each network packet is to be checked for, here each network packet is equal to a chromosome[9].

The Genetics cycle can be summarized as follows

Generation = 0

Seed population
While not (termination condition) do
Generation = generation + 1
Calculate fitness
Selection crossover
Mutation
end while[12]

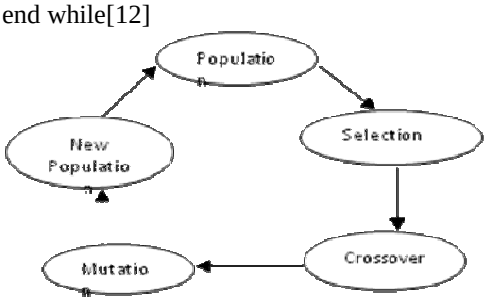

Figure 1.A basic cycle of GA

4. **Cryptography**

In general, the genetic algorithm approach has only been used to attack fairly simple ciphers.
Most of the ciphers attacked are considered to be classical[12], Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about *any* network,1 particularly the Internet. Cryptography generally use DES algorithm for the Encryption and Decryption. In DES use round and round strategy. The DES use private key and its works by using the same key to encrypt and decrypt a data, then its necessary to know both the sender and the receiver use the same private key. DES works on bits or binary numbers--the 0s and 1s common to digital computers.

5.Genetic algorithm using Cryptography

The primary goals of this work are to produce a performance comparison between traditional cryptanalysis methods and genetic algorithm based methods, and to determine the validity of typical GA-based methods in the field of cryptanalysis.
It is the most important part of encoding the data .A non repeating key guarantees better results and generates a code that is theoretically impossible to break

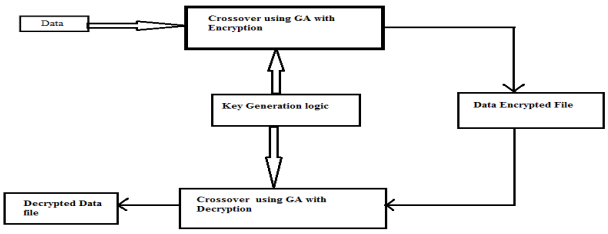

Fig 1.6 GA with Cryptography

The Genetic Algorithms cycle is illustrated in this example for maximizing a function **f(x) = x2** in the interval **0 < x <31**. In this example the fitness function is f (x) itself. The larger is the functional value; the better is the fitness of the string. In this example, we start with 4 initial strings. The fitness value of the strings and the percentage fitness of the total are estimated in Table A. Since fitness of the second string is large, we select 2 copies of the second string and one each for the first and fourth string in the mating pool. The selection of the partners in the mating pool is also done randomly. Here in table B, we selected partner of string 1 to be the 2-nd string and partner of 4-th string to be the 2nd string. The crossover points for the first-second and second-fourth strings have been selected after 1th and 2nd bit positions respectively in table B. The second generation of the population without mutation in the first generation is presented in table C [2].

Table A

Initial population and their fitness values

string no.	initial population	x	f(x)	strength fitness	(% of total)
1	01101	13	169	14.4	
2	11000	24	576	49.2	
3	01000	08	64	5.5	
4	10011	19	361	30.9	
Sum-fitness			1170	100.00	

Table B

Mating pool strings and crossover

String No.	Mating Pool	Mates string	Swapping	New population
1	01101	2	0110[1]	01100
2	11000	1	1100[0]	11001
2	11000	4	11[000]	11011
4	10011	2	10[011]	10000

Table C

Fitness value in second generation

Initial population	x	f(x) (fitness)	strength (% of total)
01100	12	144	8.2
11001	25	625	35.6
11011	27	729	41.5
10000	16	256	14.7
Sum-fitness =		1754	100.00

7. Conclusion and Future Scope

Genetic algorithms can be applied to domains in which insufficient knowledge of the system and/or high complexity is there. Genetic algorithms can find optimal solutions among the search space with the operators like crossover and mutation. Genetic algorithms are very effective techniques of quickly finding a reasonable solution to a complex problem. They are not instantaneous, but can perform an excellent search. In this work, Genetic algorithm is tested to optimize the errors of Direct Torque Control of induction motor, turbine Compressor System and DC servo motor, which shows the superiority of Genetic Algorithm than standalone soft computing controllers and conventional controllers. In future work, these techniques may be implemented for other process controllers. Other Evolutionary techniques like may further be implemented for optimisation.

References

1] Soumya Paul1, Inadyuti Dutt, S.N. Chaudhuri 1Associate Professor & Head, Asst. Professor, Dept. of Computer Application, B.P. Poddar Institute of Management & Technology, West Bengal, India, Director, Kanad Institute of Engineering & Management, West Bengal, "Implementation Of Network Security Using Genetic Algorithm", International Journal Of Advance Research in Computer Science & Software Engineering, ISSN:2277 128X,volume 3,Issue 2,February 2013.

2] Pranesh S S DEPARTMENT OF COMPUTER SCIENCE ENGINEERING. VISHVESHWARAIAH TECHNOLOGICAL UNIVERSITY, S.D.M COLLEGE OF ENGINEERING AND TECHNOLOGY. A seminar report on GENETIC ALGORITHMS 2009/10.

3] Tragha A., Omary F., Kriouile A., "Genetic Algorithms Inspired Cryptography", A.M.S.E Association for the Advancement of Modelling & Simulation Techniques in Enterprises, Series D : Computer Science and Statistics, November 2007.

4] Clark A. & Dawson Ed., "A Parallel Genetic Algorithm for Cryptanalysis of the Polyalphabetic Substitution Cipher", pages 129-138,1997.

5] Clark A., Dawson Ed. & Nieuwland H., "Cryptanalysis of Polyalphabetic Substitution Ciphers Using a Parallel Genetic Algorithm", In Proceedings of IEEE International Symposium on Information and its Applications, pages 17-20, 1996.

6] Clark a., "Modern Optimization Algorithms for Cryptanalysis", In Proceedings of the Second Australian and New Zealand Conference on Intelligent Information Systems, pages 258-262,1994.

7] Matthews R.A.J., "The use of Genetic Algorithms in Cryptanalysis", pages 187-201, 1993

8] Goldberg D.E., "Genetic algorithms in search optimization & Machine Learning", Addison-Wesley. Publishing Company, 1989..

9] L.M.R.J Lobo Professor, Department of Computer Science & Engg. Walchand Institute of Technology, Solapur, India Suhas B. Chavan MECSE (SEM IV), Department of Computer Science & Engg. Walchand Institute of Technology, Solapur, India. "Use of Genetic Algorithm in Network Security", International Journal Of Computer Application, Volume 53-No.8, September 2012.

10] S. N. Pawar Associate Professor (E &TC), Jawaharlal Nehru Engineering College, Aurangabad, MS, India," Intrusion Detection Computer Network Using Genetic Algorithm Approach : A Survey" International Journal Of Advances In Engineering & Technology, May 2013. ISSN: 2231_1963.

11] Sunil Nilkanth Pawar, Rajankumar Sadashivrao Bchkar Jawaharlal Nehru Engineering College, Aurangabad, Maharashtra State, India
G. H. Raisoni College of Engineering & Management, Pune, MaharashtraState, India. "Genetic Algorithm with Variable Length Chromosomes for Network

Intrusion Detection**".** International Journal of Automation and Computing.

12] Bethany Delman, A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Engineering ."Genetic Algorithms in Cryptography".

13] Genetic Algorithms: Concepts, Design for Optimization of Process Controllers Rahul Malhotra, Narinder Singh & Yaduvir Singh Punjab Technical University, Jalandhar, Punjab, India Tel: 91-94-6302 0007 E-mail: blessurahul@gmail.com

14] Ehab Talal Abdel-Ra'of Bader 1 & Hebah H. O. Nasereddin 2 1 Amman Arab University. 2 Middle East University, " Using Genetic Algorithm In Network".