International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.7, Special Issue.1, Jan 2019 E-ISSN: 2347-2693

A Dynamic Key Generation Scheme based on Metaheuristic Cuckoo Search

Arindam Sarkar[1*], Joydeep Dey[2], Anirban Bhowmik[3], Sk. Samim Ferdows[4]

[1] Department of Computer Science and Electronics, R.K.M. Vidyamandira, Belur Math, Belur, India
[2,4]M.U.C Women's College, B.C. Road, Burdwan, West Bengal,India, 713104
[3]Department of Computer Application, C.R.T.I., Tinkonia, Burdwan, India,713101

[*]Corresponding Author: arindam.vb @gmail.com, Tel.: +91- 9851700660

Available online at: www.ijcseonline.org

Abstract— Nature inspired food foraging features by the cuckoo species promotes the proposed methodology to generate a true random session key. To make more complex for the intruders, a key based on the behavior of cuckoo species creates the fittest solution out of the sample population. Metaheuristic based optimization algorithms are good enough to encapsulate information during the wireless communication in more secured approach. Statistical fitness function ensuring with randomized expansion of bits in the session key have been tested. The key which has been generated dynamically using cuckoo search passed through different statistical tests in order to synthesize the randomness. In this paper run test is used for examining the robustness of key and test result shows the good randomness.

Keywords - Cuckoo Search, Levy flights, Statistical tests

I. INTRODUCTION

In the era of modern information and technology, how to ensure the confidentiality of the data transmission is the biggest threat and challenge. Soft computing provides a cushion to such challenging issues with better throughputs. Cryptography is the science to encrypt and decrypt any information during network transmission. Symmetric key cryptography uses same key for both encryption and decryption purpose. While a set of key pair: { public key, private key } are used for encryption and decryption purpose respectively[1].

Metaheuristic algorithms can be used to construct session keys with more proven results. This paper presents a dynamic generation of session key based on Cuckoo Search Algorithm. In the year of 2009, Xin-she Yang and Suash Deb had effectively designed a new optimization technique i.e. Cuckoo Search Algorithm [2]. They do lay their eggs in the neighbouring nests of other birds of different species. The most interestingly the eggs laid by the cuckoos at other species nests, would be raised by surrogate parents of that species. It reduces the non raised eggs of host species and raises their population in the society. If the surrogate parents can recognize the eggs of the cuckoo, then they will either throw the alien eggs from their nests or simply reject the nest and create a new nest somewhere.

Rest of the paper has been structured as follows. Section II contains the literature survey. Problem findings are noted in the section III. The solution domain is given in section IV. Section V deals with the development of the proposed methodology to generate a dynamic session key followed by statistical tests. Result parts of this paper are given in section VI. Section VII explains the conclusion and future scope of work**.** References are listed at the end.

II. LITERATURE SURVEY

Genetic algorithm [3] is a method to solve optimization problems on natural selection criterion. The genetic algorithm repeatedly updates a sample population of solutions. At each step, the genetic algorithm selects individuals at random from the current population to become the parents for the next generation. After repeated successive generations, the sample population converges towards an optimal solution. Structural genetic representation of an optimization problem and a fitness function are the essential components of any genetic algorithm. A fitness function is used to evaluate the optimum solution at every level of generations. Following three rules are followed by genetic algorithm to generate the next level of population.

a) Selection rule: It selects the individuals, called parents, that is involved to produce the desired population at the next level of generations, which would be treated readily.

b) Crossover rule: It combines two parents to form children for the next level of population.

c) Mutation rule: It is used to effect random changes to individual parents to form children at the next generation.

The Cuckoo Search is basically satisfying the following ideal and necessary terms.

- Laying an egg at a randomly chosen visitor's nest.
- The best nests with better eggs quality (treated as session key) will move to the next generations.
- Keeping the number of host nests is fixed, and considering that a host can realize a cuckoo egg with probability PS such that $0 <= PS <= 1$. Either the host species shall break the alien egg or reject the nest, and create a new nest at a new location.

The principal searching strategy in the Cuckoo search is the use of Levy Flights [4]. A levy flight is a randomized walk for which the step lengths may be sampled in accordance to heavy tailed probability distribution. The steps tend to a stable condition after larger number of iterations.

III. PBOBLEM FINDINGS

The main problem that occurs during the transmission of data is the exchange of key in between the nodes. The key can easily be sniffed by the intruders, and hence they do synchronize with the nodes with a virtual view of being at the actual transmitter.

Another notable problem finding is the false randomness feature of the generated keys. The keys may not satisfy the stipulated ratio of the number of zeros and ones. Either such sequences are not observed in the entire sequence of bits or in the multiple blocks of homogeneous length. In case of less fitness value achieved by any key, the probability of attacks and hence chances of revealing information becomes much high.

IV. SOLUTION DOMAIN

The above noted problems noted in the section III has been addressed by the proposed methodology. Nature inspired Cuckoo search algorithm has been incorporated at our proposed methodology along with statistical analysis. Global and local searching capabilities have been explored in the Cuckoo search [2][5] with global search convergences. In addition the concept of Levy Flights is the main searching strategy in this metaheuristic searching technique to generate the optimal session key. After the generation of the session key, this would be fed into proposed statistical analyzer to test its fitness value. The fitness value in terms to random expansion of the sequence of bits. Through this analyzer, appropriate results were obtained and recorded in the results section. This favours our proposed methodology of generation of session key [6].

V. PROPOSED METHODOLOGY

Each egg present in a host nest represents a solution, and an alien cuckoo egg represents a new solution. The novelty of this proposed methodology is to find a more fit solution out of the existing solutions. If cuckoo eggs show more fitness value then host eggs would be replaced by the alien eggs in the solution set. The final solution set undergoes statistical test to find out its vulnerability in terms of the robustness. The key idea is to carry several randomness checking on the solution set [7], so that it acts as an appropriate session to resist the man in the middle attacks and geometrical attacks. Pseudo code to generate Session Key using Cuckoo Search is given below.

Algorithm 1: CuckooGenerateSessionKey(n, p_a, TC)

Input(s): Set the initial parameter $HostNetSize(n)$, $Probability(pa)$ & $Termination\ Condition(TC)$.
Output(s): The best keystream (solution) as a session key
Method(s): Each gene is generated by either double stepping or addition of last two genes or adding random gene with the last gene .Among these 3 methods one method is used each time depends on probability value.

1: Set $t := 0$ {/*Counter initialization */}
{/*Initial population of keystream */}
2: for i = 1 to i <= n do
3: Generate an initial population of n keystream $(host)\ x_i^t$
4: Evaluate the fitness function for each $keystream\ (host\ \ egg) f(x_i^t)$
5: end for
6: repeat
7: Generate a new $keystream\ (Cuckoo)\ x_i^{t+1}$ as randomly by levy flight.
8: Randomly choose a nest x_j among n solutions.
9: Checkif ($f(x_i^{t+1}) < f(x_j^t)$)
10: Put back : Solution x_j with the solution x_i^{t+1}
11: End Checkif
12: Abandon a fraction p_a of worse nest
13: Build new nest at new location using Levy flight a fraction p_a of worse nest
14: Save the best solution and find the current best solution
15: set $t \leftarrow t + 1$
16: until $t < TC$
17: produce the best $keystream\ (solution)$

The above stated algorithm 1 generates the optimal session key. Now this keystream would be tested statistically to find the randomness in nature. If this test converges to success then this session can be used by the nodes to encrypt any data before transmission. It minimizes the chances to decipher the text by the intruders for data manipulation or distortion. The pseudo code for such statistical test is given in the following algorithm 2. The standard efrc( ) [8] has been used at the following algorithm.

Algorithm 2: StatisticalParseAnalyzer(Keystream [Size])

Input: - Integer Array: $StBits[Size]$; Fittest Key Stream
Output: - $p - value$ ($StBits[Size]$) ; Probability Value

1. Set $num\_ones, prop, x, y \leftarrow 0.0$;
2. Set $r, j \leftarrow 0$
3. for $i = 0\ to\ Size$ do
4. if($StBits[i].Equals$ (1))
5. $num\_one \leftarrow num\_one + 1$
6. end if
7. prop← $(num\_one * 1.0)\ /\ Size$
8. end for
9. for $j = 0\ to\ Size$ do
10. if ($StBits[i].NotEquals(StBits[i+1])$)
11. $j \leftarrow j + 1$
12. end if
13. end for
14. x= $ABS(r - (2 * Size * prop * (1 - prop))$
15. y=2 $* (sqrt(2.0 * Size) * prop * (1 - prop))$
16. p-value← Call $erfc(x/y)$
17. $Return\ p - value$

VI. RESULTS SECTION

In the result section we use statistical test such as run test for checking randomness of key. The results obtained from the proposed methodology has been tested and compared with classical existing encryption algorithm standards.

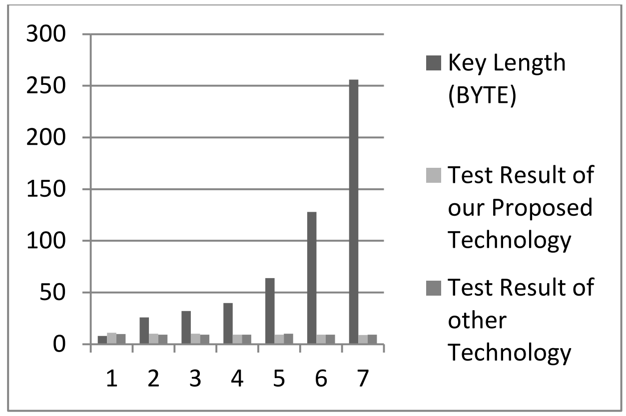
Table 1: Data set for Runs Test

Key size (BYTE)	Test Result of our proposed technology	Test Result of other technology
08	11.0928	9.9339
16	10.2876	9.1235
32	9.3254	9.1345
40	9.2872	9.2144
64	9.1672	9.2134
80	9.1104	9.2378
128	9.3852	9.2564
150	9.5274	9.2618
200	8.6870	9.2834
256	8.6764	9.3802

Depending upon the different ranges of the key size measured in bytes, the following table 3 contains the data set for statistical test. In most of the cases of the key length, the proposed technology shows favourable outcomes in terms of true randomness.

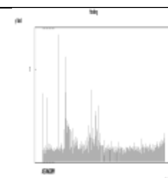
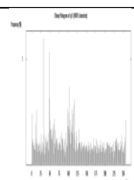
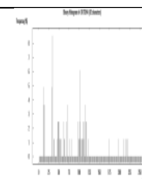
When the key size is 8 bytes, then the proposed technique gives 9.9339 which is satisfactory with respect to 11.0928, for other standard technique. Doubling the key size to 16 bytes the proposed technique shows better results in the form 9.1235. In case of 32 bytes key length, at par results have been obtained as 9.2345. Acceptable results were found at extreme large key size of 40 bytes having value of 9.2434.

Figure 1 : Bar Chart for Statistical tests



ANALYSIS OF HISTOGRAM

Table 2 : Histogram Comparison

TOOLS	PLAIN TEXT	DATA ENCRYPTION STANDARD	PROPOSED TECHNIQUE
HISTOGRAM			

From table 2, it can be said that the histogram of our proposed methodology provides better results with respect to plain text, and showing at par histogram with respect to standard encryption techniques such as DES [9][10].

ANALYSIS OF FLOATING POINT FREQUENCY:

Table 3 : Floating Point Frequency Comparison

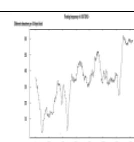
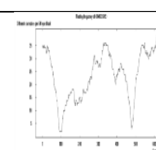
TOOLS	PLAIN TEXT	DATA ENCRYPTION STANDARD	PROPOSED TECHNIQUE
FLOATING POINT FREQUENCY			

Table 3 shows the floating point frequencies comparison between the plain text, standard encryption method, and proposed technique. The floating point frequencies graph of our proposed technique denotes better results as compared to auto correlation of plain text, and existing standard encryption techniques such as DES.

VI. CONCLUSION AND FUTURE SCOPE

The global searching converging logic is satisfied in the session key generated by the cuckoo search. In addition, the session key thus generated has been statistically tested with the ratio of uniformity in bits sequence. The favourable results obtained from the tests tend to accept our proposed methodology. Hence, the proposed key generation is suitable for both symmetric and asymmetric encryption. It is hard to decrypt the session key by the intruders due to its absolute randomness.

Future scope is to implement multi-variate Cuckoo search based key generation in asymmetric key encryption. Now in both symmetric and asymmetric key encryption our method is very useful because of its dynamic flavour. Different types of banking applications, share markets and in case of secure file transmission, our method would be applicable.

REFERENCES

[1]. Younsung Choi, Cryptanalysis on Privacy-Aware Two-Factor Authentication Protocol for Wireless Sensor Networks, Indonesian Journal of Electrical Engineering and Computer Science Vol. 8, Issue 2, pp. 296 – 301, 2017

[2]. Xin-She Yang, Suash Deb, Cuckoo Search via Levy Flights, In the Proceedings of the 2009 World Congress on Nature & Biologically Inspired Computing (NaBIC 2009), IEEE Publications, USA, pp.210-214, 2009.

[3]. T. El-Ghazali, Metaheuristics: From Design to Implementation, vol. □□, John Wiley & Sons, □□□

[4]. T. El-Ghazali, Metaheuristics: From Design to Implementation, vol. □□, John Wiley & Sons, □□□

[5]. Gove Nitinkumar Rajendra, Bedi Rajneesh kaur , "A New Approach for Data Encryption Using Genetic Algorithms and Brain Mu Waves", International Journal Of Scientific And Engineering Research Volume 2, Issue 5, May-2011.

[6]. Baumjohann, W., and R. A. Treumann (1997), Basic Space Plasma Physics, Imperial College Press, London.

[7]. Abramowitz, M., and I. A. Stegun (1965), Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables, Dover.

[8]. Iztok Fister Jr., Dusan Fister, Iztok Fister, A comprehensive review of cuckoo search: variants and hybrids, Int. J. Mathematical Modelling and Numerical Optimisation, Vol. 4, Issue. 4, pp.387-409, 2013.

[9]. 7.C.Asmuth and J.Bloom, A modular to key safeguarding, IEEE Transaction on Information Theory, vol.29, no. 2, pp. 208-210, 1983.

[10]. G.R. Blakley, Safeguarding cryptographic keys,in Proceedings of AFIPS International Worhshop on Managing Requirements Knowledge, pp. 313, 1979.

[11]. Whitfield Diffman and Martin Hellman New Directions of cryptography, Bulletin of the American Mathematical Society 42 (2005), 3-38; online in 2004. ISSN 0273-0979.

[12]. M. L Wu and T. Y. Hwang, 1984, Access control with single key-lock, IEEE Transaction on Software Engineering, Vol. SE- , No. 2, pp.185-191.

Authors Profile

ARINDAM SARKAR is currently serving the Deparment of Computer Science & Electronics, Ramakrishna Mission Vidyamandira, Belur Math-711202, Howrah as an Astt. Professor. He has completed his Master of Computer Application (M.C.A) degree in the year of 2008 from VISVA BHARATI, Santiniketan, WB, India and he secured University First Class First Rank. In the year of 2011, Dr. Sarkar has completed his M.Tech in Comuter Science & Enggineering degree from University of Kalyani, WB, India and also secured University First Class First Rank. Dr. Sarkar has completed his Doctor of Philosophy in Engineering in the year of 2015 from University of Kalyani under the INSPIRE Fellowship Scheme of Department of Science & Technology (DST), New Delhi, India. In the year of 2016 he has secured 2nd Rand in the West Bengal College Service Commission examination. He has more than 50 International Journal and Conference publications.

Joydeep Dey pursed Bachelor of Computer Application (Honours) from Cyber Research & Training Institute, Burdwan, India in 2007 and Master of Computer Application from the University of Burdwan in year 2011 with first class first rank. He is working as Leturer in Department of Computer Sciences at M.U.C. Women's College, Burdwan West Bengal, India since 2011. He has published two conferences papers and it's also available online. His main research work includes Cryptography and Computational Intelligence.. He has 7.5 years and 0.5 years of teaching experience at UG and PG level respectively.

Anirban Bhowmik completed Bachelor of Science(Mathematics) from Bolpur College, Bolpur, West Bengal, India and Master of Computer Application from the University of Burdwan in year 2008. He is working as an Assistant Professor in Department of Computer Application at Cyber Research & Training Institute, Burdwan West Bengal, India since 2008. He has published two international conferences papers and it's also available online. His main research work focuses on Cryptography and Soft Computing. He has 10 years of teaching experience at UG level.

Sk. Samim Ferdows teaches Statistics at M.U.C Women's College, Burdwan, West Bengal. He is a Doctorate from University of Burdwan. He has 21 publications in different national and international journals. He has research interest in Quantitative methods, Statistics and Econometrics.