ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Vol. 5, Issue 1, Januray 2016

A Survey on Network Security Using Genetic Algorithm

Subhrajit Mondal[1], Tania Khatun Mollah[2], Arindam Samanta[3], Soumya Paul[4]

Student, Master of Computer Application, B.P. Poddar Institute of Management & Technology, West Bengal, India1

Student, Master of Computer Application, B.P. Poddar Institute of Management & Technology, West Bengal, India[2]

Student, Master of Computer Application, B.P. Poddar Institute of Management & Technology, West Bengal, India[3]

Associate Professor and Head, Department of Computer Application, B.P. Poddar Institute of Management & Technology, West Bengal, India[4]

ABSTRACT: As the internet evolves and computer networks become bigger and bigger, network security has become one of the most important factors for companies to consider. This paper concerns about the security of confidential information and data transmission using symmetric key cryptography with Genetic Algorithm in order to provide confidentiality, authentication, integrity and non-repudiation of the messages. First, an encryption algorithm is developed and implemented to achieve the aforementioned purpose. A plain text is encrypted using privet key, taken as input from user, to produce an intermediate cipher. The intermediate cipher is again encrypted using genetic algorithm to produce final cipher. The final cipher first decrypted to produce the intermediate cipher which in turn decrypted to get the plain text using the Private Key.

KEYWORDS: Symmetric-Key, Network Security, Genetic Algorithm.

I. INTRODUCTION

A. Network Security

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 resource. Network Security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned a password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everybody jobs conducting transactions and communications among business, government agencies and individuals.

B. Genetic Algorithm

Genetic algorithms are inspired by Darwin's theory about evolution. Solution to a problem solved by genetic algorithms is evolved. Algorithm is started with a set of solutions (represented by chromosomes) called population. Solutions from one population are taken and used to form a new population. This is motivated by a hope, that the new population will be better than the old one. Solutions which are selected to form new solutions (offspring) are selected according to their fitness - the more suitable they are the more chances they have to reproduce. This is repeated until some condition (for example number of populations or improvement of the best solution) is satisfied.

C. Symmetric key

Symmetric key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plain text and decryption of cipher text.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Vol. 5, Issue 1, Januray 2016

II. RELATED WORK

1. Stamatios V. Kartalopulos focuses on cryptography and security in communicators, wireless and IP network security, as well as optical network security, quantum cryptography and quantum-key distribution processes specific to optical networks is discussed.
2. Rex Maced Arokiarai, A.Bannari, Sathyamana Glam Shanmngam proposed in this paper, description of the framework to solve the security threats by designing and address based cryptography scheme, An address based cryptography scheme(ACS) as a combination of ad-hoc address and public key cryptography. ACS is a certificate less public key cryptography solution in that public keys of mobile nodes are directly derivable from their known ad-hoc node address plus some common information. Thus it eliminates the need for certificate based authenticated public key distribution essential in conventional public key management schemes. ACS is an efficient construction method of address based public/private keys cryptography, which not only ensures high level authentication to node exchange information, but also enables efficient network-wide secure key update via a single broadcast message.
3. A. Tragha described a new symmetrical block ciphering approach named ICIGA (Improved Cryptography Inspired by Genetic Algorithms) where session key is generated in a random process. ICIGA is an enhancement of the system (GIC) ―Genetic algorithms Inspired Cryptography.

III. THE DESIGN

The proposed has followed the following phases-

i. Text Matrix generation using ASCII value.
ii. Key Matrix generation using reverse QWERTY keyboard wise positional value.

TABLE 1

M	N	B	V	C	X	Z	L	K
1	2	3	4	5	6	7	8	9
J	H	G	F	D	S	A	P	O
10	11	12	13	14	15	16	17	18
I	U	Y	T	R	E	W	Q	
19	20	21	22	23	24	25	26	

iii. Matrix subtraction.
iv. Matrix substitution using function.
v. Genetic crossover, mutation and inversion.

IV. ALGORITHM

Input: Message, Private Key
Process: Plain text is converted into a cipher text using a key
Output: Message

A. Algorithm for encryption

Step 1: Convert each character of message into its corresponding ASCII value and store it in a matrix.
Step 2: Take the reverse QWERTY keyboard wise positional value of each character of password and store it in a matrix.
Step 3: Subtract password matrix from message matrix and get a new subtracted matrix.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Vol. 5, Issue 1, Januray 2016

Step 4: Create a substituted matrix using function: (ax-b)*c where a,b,c are random variables and x is subtracted matrix.
Step 5: Convert the 1st and last elements of substituted matrix into binary form and consider it as intermediate cipher.
Step 6: Perform Crossover operation on those two binary strings and take the decimal values of these.
Step 7: Add these two decimal numbers and again convert it into binary form.
Step 8: Perform Mutation operation on it.
Step 9: Perform Inversion operation on it, and then convert the binary no into its equivalent decimal no.
Step 10: Now take each digit of this no and take its reverse QWERTY keyboard digit. It will be the final cipher.
Step 11: Exit.

B. Algorithm for decryption

Step 1: Take reverse QWERTY keyboard positional value of final cipher and convert it to binary no.
Step 2: Perform Inversion operation.
Step 3: Perform Mutation operation, convert it into decimal no.
Step 4: Get back two distinct decimal numbers and perform Crossover operation on the binary form of these two numbers.
Step 5: Fetch the substituted matrix using the numbers.
Step 6: Get back the subtracted matrix using reverse function.
Step 7: Add password matrix and get message matrix.
Step 8: Fetch the characters of message.
Step 9: Exit.

C. Proposed security algorithm

Step 1: A plain text is taken as input in source end.
Step 2: Call algorithm for encryption
Step 3: Cipher text is generated.
Step 4: Call algorithm for decryption
Step 5: Plain text is received at destination.
Step 6: Exit.

V. EXAMPLE ILLUSTRATION

A. Example Illustrating Encryption Algorithm

- Text matrix generation:

Plain text - ANDROID
Corresponding matrix in ASCII –

65	78	68
82	79	73
68	32	32

(Empty spaces of the matrix will be occupied by 32, which is the ASCII value for ‘blank’)

- Key matrix generation:

Private Key - BPPIMTMCA

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Vol. 5, Issue 1, Januray 2016

Corresponding matrix using reverse QWERTY keyboard wise positional value –

3	17	17
19	1	22
1	5	16

- Subtracted matrix generation:

Subtract key matrix from text matrix to achieve the following -

62	61	51
63	78	51
67	27	16

- Substituted matrix generation:

New matrix using function (ax-b)*c
(a, b, c = Random Variables)
(x = Subtracted matrix)
(Here a=2,b=17,c=3)

214	210	170
218	278	170
234	74	30

- Intermediate cipher:

Convert into binary the 1st and last value of previous matrix

1101 0110
0001 1110

- Genetic Crossover:

Crossover operation ---

1101 1110
0001 0110

Decimal value of new strings -

222 & 22

Sum - 244
Again in binary - 1111 0100

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

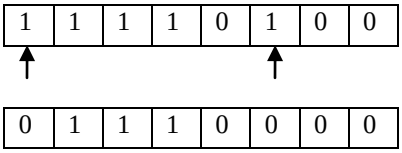
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Vol. 5, Issue 1, Januray 2016

- Genetic Mutation:

Mutation operation ---



- Genetic Inversion:

Inversion operation ---

1000 1111

Equivalent decimal value: 143

- Final Cipher: MVB

(1 – M, 4 – V, 3 – B (using reverse QWERTY keyboard wise positional value))

B. Example Illustrating Decryption Algorithm

Final Cipher - MVB
Extracted decimal value – 143
Equivalent binary number - 1000 1111

After Inversion operation - 0111 0000

After Mutation operation - 1111 0100

Decimal value - 244
Different numbers - 222 & 22
Binary form -

1101 1110
0001 0110

After Crossover operation -
(It is the intermediate cipher)

1101 0110
0001 1110

Now the matrix –

214	210	170
218	278	170
234	74	30

After applying reverse function of (ax-b)*c :

62	61	51
63	78	51

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Vol. 5, Issue 1, Januray 2016

67	27	16

Text matrix –
(After adding the key matrix from previous matrix)

65	78	68
82	79	73
68	32	32

Finally we get the text using ASCII value –

ANDROID

VI. CONCLUSIONS

In this work, network security using genetic algorithm in computer networks has been proposed. A symmetric cryptographic approach using mathematical function has been implemented to ensure confidentiality in computer networks, which is again designed with genetic algorithm.

REFERENCES

[1] Sindhuja k,Pramela Devi S, A Symetric Key Encryption Technique Using Genetic Algorithm Vol:-5(1),2014,414-416 (IJCSIT) ISSN-0975-9646
[2] Vulnerabilities and Security strategy for the Next Generation bandwidth Elastic Pon Stamatios V.Kartalopous,Di Jin Ece department,TCOM Graduate program, The University of Oklahoma, 4502 E.41 st Street,Tulsa,OK 74135 USA.
[3] Kartalopoulos, S.V. "Differentiating Data Security and Network Security", IEEE Communications, 2008. ICC"08. International Conference on Telecommun. Networking, Univ. of Oklahoma, Tulsa, OK, pp. 1469 – 1473, Issue Date: 19-23, May 2008.
[4] Stamatios V. Kartalopoulos, Williams Professor in Telecommunications Networking, "Optical Network Security: Countermeasures in View of Channel Attacks", Military Communications Conference,
2006. MILCOM 2006. IEEE, The University of Oklahoma, Washington, DC, ISBN: 1-4244-0617-X, pp. 1-5, Issue Date: 23-25 Oct, 2006.
[5] Douglas, R.Stinson, "Cryptography – Theory and Practice", CRC Press,1995
[6] David E Goldberg, "Genetic algorithms in search, optimization and machine learning", Addition – Wesley, 1989
[7] Subhranil Som, Niladri Shekhar Chatergee, J.K. Mandal, "Key Based Bit Level Cryptographic Technique(KBGCT)", 7th International Conference on Information Assurance and Security, 2011
[8] A. Tragha, F. Omary, A. Kriouile, "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 2005.
[9] A. Tragha, F. Omary, A. Mouloudi, "Improved Cryptography Inspired by Genetic Algorithms", ICIGA, 2006 International Conference on Hybrid Information Technology (ICHIT'06).
[10] Soumya Paul, et.al ―Design and Implementation of Network Security using Neural Network Architecture‖, Journal of Computing Vol 4, Issue: 8 August 2012, pp 115-120, ISSN: 2151-9617.
[11] Dr. Soumya Paul et al, Implementation of Network Security Using Neural Network Architecture, Vol.4 Issue.6, June- 2015, pg. 815-821
[12] Soumya Paul et.al ,Implementation of Network Security Using Genetic Algorithm ,Vol 3 Issue 2,February-2013 ISSN:2277-128X
[13] Cryptography and Network Security, by Forouzon.
[14] William Stallings, Cryptography and Network Security, 2nd edition.
[15]

BIOGRAPHY

Subhrajit Mondal, pursuing Master's Degree in Computer Application (Final year), holds a bachelor's degree in Computer Application (Hons.) from University of Burdwan.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly Peer Reviewed Journal)

Vol. 5, Issue 1, Januray 2016

 **Tania Khatun Mollah**, pursuing Master's Degree in Computer Application (Final year), holds a bachelor's degree in Computer Science (Hons.) from University of Calcutta.

 **Arindam Samanta**, pursuing Master's Degree in Computer Application (Final year), holds a bachelor's degree in Computer Application (Hons.) from University of Burdwan.

 **Dr. Soumya Paul,** Assoc. Professor and Head, Department of Computer Application in B. P. Poddar Institute of Management & Technology, Kolkata, has been in teaching and research for over 15 years. He holds a Master's Degree in Technology, Computer Application as well as in Mathematics and has gathered vast experiences in the same. He received his M.Sc. (Mathematics) from Visva Bharati University and stood 1st class 1st. He received MCA from National Institute of Technology, Rourkela and M. Tech (CSE) from AAI-Deemed University and has Ph. D in Computer Science and Engineering. He served as a faculty member and guest faculty member in various Institutes and Universities like RCCIIT, Visva Bharati University, University of Calcutta, University of Burdwan, Maulana Abul Kalam Azad University of Technology, Assam University-Silchar etc. He has delivered numerous lectures across India in the field of his research interest, Optical Networks and Genetic Algorithms. He is an author, co-author of several published articles in International Journals and International Conferences, book. He has chaired an International Conference technically supported by IEEE communication in corporate institute of Science and Technology, Bhopal. He has more than 26 research publications and currently Reviewer and Member, Editorial Board in International Journals.