ISSN: 2250-3676
Volume-3, Issue-2, 62-66

A NOVEL APPROACH FOR NETWORK SECURITY IN WDM

Soumya Paul[1], Inadyuti Dutt[2], S.N. Chaudhuri[3]

[1]Assoc. Professor, Department of Computer Application, B. P. Poddar Institute of Management & Technology, West Bengal, India, ***soumya.paul2000@gmail.com***

[2]Asst. Professor, Department of Computer Application, B. P. Poddar Institute of Management & Technology, West Bengal, India, ***inadyuti@gmail.com***

[3]Director, Kanad Institute of Engineering &Management, West Bengal, India, ***satya.chaudhuri@rediffmail.com***

Abstract

Abstract: All-optical networks are able to transport a huge amount of traffic with fast data rates, but it brings a set of new challenges towards the network operator in terms of network security. One of them is secure transmission of information without compromising data integrity and confidentiality. In this paper an asymmetric cryptographic algorithm (Public-key cryptography) is implemented with Genetic Algorithm to ensure the confidentiality issue in a transparent all-optical network (AON).

Index Terms*: All-optical network (AON), Public-key cryptography, Genetic Algorithm (GA)*

1. INTRODUCTION

In an all-optical network (AON), all network-to-network interfaces are based on optical transmission, all user-to-network interfaces use optical transmission on the network side of the interface and all switching and routing within AON network nodes is performed optically. The main characteristic of AONs is to provide transparency, which is very advantageous for high data rate communications or rapidly changing environments. But it brings onward a set of new challenges in terms of network security. One of the serious problems with network transparency is that the properties of transparent optical components make AONs particularly vulnerable to various forms of attacks. As the network transports a massive aggregate traffic, therefore, the issues of information privacy become very important along with network security. Different methods have been developed to assure that only the sender and the receiver would be able to read a message, while it would be unreadable to a third party. Public-key cryptography allows users to communicate securely using a pair of keys, one that is public and the other is private, without having prior access to a shared secret key; these two keys are not independent but are mathematically related [5]. In this paper an asymmetric cryptographic approach (Public-key cryptography) is implemented with Genetic Algorithm (GA) to ensure the confidentiality issue in a transparent all-optical network (AON).

The paper provides proposed heuristic in section 2. Simulation and results are given in section 3. Finally the paper concludes in section.

2. PROPOSED HEURISTIC

The proposed heuristic is implemented using GA. The heuristic contains encryption algorithm and decryption algorithm.

2.1. Problem Definition

The sender's message (plaintext) will be converted into illegible form (cipher text) without any loss of text by using encryption algorithm. At the receiver side the unreadable text is deciphered using decryption algorithm and the recipient will get the original message (plaintext).

2.2. Algorithms

2.2.1. Encryption Algorithm

Input: Plaintext
Output: Cipher text

1. Compute the length of the entire plaintext or message (msg-len) including blank spaces and punctuations.

a. Compute temp1= ceiling value of (msg-len/n), where n is number of bits in a block.

b. Calculate m= msg-len mod n,

If m≠0,

If, temp1 is even,

add (temp1*n – msg-len) number of extra spaces at the end of the plaintext. Here the Population size is equal to temp1.

Else, add ((temp1*n – msg-len)+n) number of extra spaces at the end of the plaintext. Here the Population size is equal to temp1+1.

Else,

If, temp1 Is even,

No extra space is required to add. Population size is equal to temp1.

Else, add only n number of extra spaces at the end of the plaintext. Population size is equal to temp1+1.

c. Initialization:

ISSN: 2250-3676
Volume-3, Issue-2, 62-66

Set generation number t ← 1; Set maximum generation max_gen ← 100; Set string length xlen ← n; Set crossover probability pcross ← 0.99; Set mutation probability pmut ← 0.99;

d. Initial population (ini_pop):

Divide the plaintext (output of step 3) into n-bit blocks. Each block is a string of initial population. The total number of blocks is equal to population size.

e. Fitness function :

$fit(S_i)=\sum_{i=1}^{BL} \delta$

BL=length of each block.

${}^{b}\delta_i$ =Boolean variable, takes value 1 if i^{th} bit of b block is matched with j^{th} bit of the plaintext, where j=n *(b-1) +i. otherwise takes value 0.

7. Crossover:

The crossover operation is described below on the strings of ini_pop and obtains a population of new_pop of size pop_size and the strings are arranged according to its original block number.

a) Randomly select two strings as pair from ini_pop such that the total number of each string is equal to the corresponding actual count and form (pop_size/2) number of paires.

b) Crossover site (xsite) = approximate value of mean of mate numbers.

If xsite> n-1, then xsite =remainder of (calculated xsite/(n-1)).

c) Generate a random number r_k from [0, 1] for k= [1, 2… (pop_size/2)] for each pair such that, if $r_k \leq$pcross, the crossover will undergoes at the cut point xsite.

8. Compute fit (S_i) for each string S_i ($1 \leq i \leq$pop_size) of new_pop.

if, $\sum$ fit (S_i) of new_pop> $\sum$ fit (S_i) of ini_pop,

a) then the strings of ini_pop are kept in temp_pop. b) Go to step 9.

else

if t< max_gen,

a) Set t←t+1; b) Rename new_pop as ini_pop; c) Go to step 7.

9. Mutation:

Mutation operation is described below on the string of temp_pop and obtains a population final_pop of size pop_size.

Generate a random number r_m from [0, 1] for m= [1, 2… pop_size] for each 1st node of each string S_i ($1 \leq i \leq$pop_size) of final_pop such that,

if $r_m \leq$pmut, exchange 1st node of S_i with any oth randomly selected node n_k of S_i where $1 \leq k \leq$xlen and $k \neq 1$.

10. The strings (blocks) of final_pop are placed according to the generated random number r ($1 \leq r \leq$pop_size) and return it as cipher text.

2.2.2. Decryption Algorithm

Input: Cipher text
Output: Plaintext

1. Compute the length of the entire cipher text or message (msg-len) including blank spaces and punctuations.
2. Population size (pop_size) = (msg-len/n), where n is number of bits in a block.
3. Initial population (ini_pop): Divide the cipher text into n-bit blocks. Each block is a string of initial population. The total number of blocks is equal to population size. The blocks or strings of ini_pop are rearranged with the help of random number generated in

Key : The key contains i) value of n, ii) block-numbers (mate-numbers) for crossover, iii) randomly generated node number for mutation and iv) numbers generated for random arranged of the blocks.

Decryption algorithm: Extra spaces are not required here to produce initial population or to adjust population size. The blocks are again rearranged and mutation operation is performed according to the information mentioned in the key. The notable thing is here we don't need to compute fitness value of any block as we already know the number of generation from the key. After crossover (as mentioned in the algorithm) we can easily get the original message (plaintext).

2.2.4. Example illustrating proposed heuristic

We have taken a simple example to illustrate the proposed heuristic. Plaintext: 'Message cannot be displayed here.' Here message length (msg-len) =33. Considering n=6, population size (pop_size) = 6. Here extra three blank spaces required to add at the end of the plaintext. Table 1 shows initial population and its fitness value.

String No.	Initial population						fit(S_i)
1.	M	e	s	s	a	g	6
2.	e		c	a	n	n	6
3.	o	t		b	e		6
4.	d	i	s	p	l	a	6

ISSN: 2250-3676
Volume-3, Issue-2, 62-66

5.	Y	e	d		h	e	6
6.	R	e	.				6

Table- 1: Fitness value of each string

al fitness value= 36
e considerations are:
Population size (pop_size) = 6; (ii) Maximum number of generation ax_gen) = 100; (iii) String length =n=6; (iv) Crossover probability (pcross) .99; (v) Mutation probability (pmut) =0.99;

le 2, 3 and 4 show crossovers and generation of new populations.

Mate-numbers	Xsite	New population (new_pop)	fit(S_i)
(1,4)	3	M e s p l a	3
		e c a h e	4
(2,5)	4	o t b e	6
		d i s s a g	3
(3,6)	5	y e d n n	4
		r e .	6

Table- 2: Generation 1, Total fitness value=26<36

Mate-numbers	Xsite	new_pop	fit(S_i)
(4,3)	4	M e c a h e	2
		e s p l a	2
(2,1)	2	o t b a g	4
		d i s s e	3
(5,6)	1	y e .	3
		r e d n n	3

Table- 3: Generation 2, Total fitness value=17<26

Mate-numbers	Xsite	new_pop	fit(S_i)
(1,6)	4	M e c a n n	2
		e s p	2
(5,2)	4	o t b e	6
		d i s s a g	3
(3,4)	4	y e . l a	3
		r e d h e	3

Table- 4: Generation 3, Total fitness value=19>17

As total fitness value of the strings of generation 3> total fitness value of the strings of generation 2, we will not go to the next generation and take the strings (new population) of generation 2.

Table 5 describes mutation operation where the 1st bit of each string of temp_pop is exchanged with the node n_k and produce final_pop.

temp_pop	n_k	final_pop
M e c a h e	3	c e M a h e
e s p l a	2	e s p l a
o t b a g	5	a t b o g
d i s s e	5	e i s s d
y e .	3	. e y
r e d n N	4	e d r n n

Table- 5: Mutation

The strings (blocks) of final_pop are arranged accordin to thefollowing number – 6, 2, 1, 3, 4, 5. Finally the cipher text is: ‘ edrnn esplaceMaheat bogeissd .ey ’

(If ‘blank spaces’ are replaced by ‘*’ then the cipher text is: ‘ *edrnn*esplaceMaheat bogeissd*.ey***’).

To decipher the encrypted message at first the message-length is divided by n and the generated blocks are rearranged (the 1st block will be placed in 6th position, the 2nd block in 2nd position, 3rd block in 1st position, 4th block in 3rd position, 5th block in 4th position and finally 6th block in 5th position) and we will get same string as the strings of final_pop in table 5. Next mutation is performed reversely on these strings and the strings of temp_pop of table 5 will be generated. Crossover for 1st generation will be performed on these strings (same mate-numbers and xsite as in table 3) and strings of new_pop of table2 will be produced. Similarly, crossover for 2nd generation will be performed on these strings (same mate-numbers and xsite as in table 2) and strings of ini_pop of table1 will be generated. After sequential placing of these strings the original message (plaintext) can be obtained.Another example considering n=10

At the sender site-

Plaintext: 'Good Morning. We have arranged a function on next Sunday at the evening. We are requesting you to please come and join with us. Thank you.'

ISSN: 2250-3676
Volume-3, Issue-2, 62-66

Cipher text: ‘ non s.gT hg.frnextnu d aou.iova W erndnundyaSgenoah tr pl y Wjoine se e cort eodun ni hea Momeistqueiting .oue aaet nk eenhav oarayctGw’

At the receiver site-

Cipher text: ‘ non s.gT hg.frnextnu d aou.iova W erndnundyaSgenoah tr pl y Wjoine se e cort eodun ni hea Momeistqueiting .oue aaet nk eenhav oarayctGw’

Plaintext: 'Good Morning. We have arranged a function on next Sunday at the evening. We are requesting you to come and join with us. Thank you.'

3. SIMULATION AND RESULTS

The cipher text of same message with same n value can produce different text.

Plain text: 'message cannot be displayed here.'

Cipher text: ‘eispd .ey necamns esagto bla edrhe’

Cipher text:‘ ispldatssogc eaheem be dey nnae. r’

In both the cases the value of n=6.

4. CONCLUSION

In this work, an asymmetric cryptographic algorithm is implemented with genetic algorithm. The proposed heuristic ensures confidentiality, authenticity in a transparent all optical network and the simulation portray the results.

REFERENCES

[1] Vulnerabilities and security strategy for the Next Generation Bandwidth Elastic PON STAMATIOS V. KARTALOPOULOS, DI JIN ECE Department and TCOM graduate program The University of Oklahoma, 4502 E. 41st Street, Tulsa, OK 74135 USA.

[2] A New Approach to Optical Networks Security: Attack-Aware Routing and Wavelength Assignment Nina Skorin-Kapov Member, IEEE, Jiajia Chen, Lena Wosinka, Member, IEEE.

[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] Cryptography and Network Security, Third Edition, by William Stallings.

[5] Cryptography and Network Security (Sie), by Forouzan.

[6] An introduction to Neural Networks, by Kevin Gurney, Kevin N. Gurney.

BIOGRAPHIES

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 12 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, Rourkella and M. Tech (CSE) from AAI-Deemed University and pursuing Ph. D in Computer Science and Engineering. He served as a faculty member and visiting faculty member in various Institutes and Universities like RCCIIT, Visva Bharati University, University of Calcutta, Bardhaman University, West Bengal University of Technology 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. He has chaired an International Conference technically supported by IEEE communication. He has more than 26 research publications and currently Reviewer and Member, Editorial Board in many conferences and journals like International Journal of Data Modeling and Knowledge Management.

I**nadyuti Dutt**, has been in the field of academics and research for more than ten years and is currently the Assistant Professor in the Department of Computer Application of B. P. Poddar Institute of Management & Technology, Kolkata, West Bengal, India. .Earlier, she held several technical positions in

ISSN: 2250-3676
Volume-3, Issue-2, 62-66

National Informatics Centre, Kolkata and Semaphore Computing Networks Pvt. Ltd. respectively. She has earned Master's Degree in Computer Application and currently pursuing her research in Computer Science and Engineering. She has more than 26 publications to her laurels and her research interest is specifically in the field of Optical Networking, Security and Genetic Algorithms.

She has also been Member, Editorial Board in journal publicationss like International Journal of Software Engineering & Research.

Prof. Dr. S.N. Chaudhuri, Director, Kanad Institute of Engineering & Management, Manakar, Burdwan, West Bengal. He is a renowned Academician as well as Scientist. He has a working experience for nearly40 years in different National and International Institutions. As a visiting Professor, he visited different foreign Universities. He has numerous publications to his laurels and his name has been included in Who is Who Indian Personages.