ISSN: 0975-766X
CODEN: IJPTFI
Available Online through ***Review Article***
www.ijptonline.com

SPANNING TREE APPROACH FOR ERROR DETECTION AND CORRECTION

Chandra Segar Thirumalai[1], Senthil Kumar M[1]
[1]Assistant Professor Senior, School of Information Technology and Engineering, VIT University, Vellore, India.
Email: chandru01@gmail.com

Received on 10-10-2016 *Accepted on: 20-11-2016*

Abstract:

This research based paper's focus is to develop a spanning tree approach for error detection and correction in the data being received at the receiver's portal. The main objective of this paper is to ease the error detection process inculcated in the data received from a reliable source. The main contribution of this paper is the development of error detection algorithm which is integrated on Spanning Tree approach. Spanning tree (say T) is a tree composed of all the vertices and some edges of a connected, undirected graph(say G) where in every vertex lies in the tree but no cycles(or loops) are formed. The technique being used in the paper will help find the errors that are usually encountered during the transmission of the data unit. The traditional correction techniques are being coupled with the newly proposed method to attain the error-free data unit.

Keywords: Spanning tree, error detection and correction

1. Introduction

In the networking scenario, a reliable delivery of data from the sender's port to the receiver's port over communication channels is needed. But these communication channels are prone to channel noises, which leads to error in the data during the transmission from the source to a receiver. An error is nothing but any change or mismatching that takes place between the data unit sent by the transmitter and the data unit being received at the terminal. The error detection and correction techniques enable the delivery of the desired result, that is, the correct data unit at the terminal. The error detection technique helps to determine the error which might have occurred during the transmission like one caused by noise or by other impairments. The error correction methodology includes or involves reconstruction of the data which is being tampered or detected with error.

In this paper, the spanning tree approach is implied on the data being sent and received over a network. A spanning tree (say T) is a tree which consists of all the vertices and some edges of a connected, undirected graph (say G), or in other words, we can say that it is a tree of a connected graph, with maximal set of edges of G containing no cycle or minimal set of edges which connects all the vertices of G. For any given connected undirected graph with V vertices, will form a spanning tree with V vertices and V-1 edges. In graph theory, many optimization problems are being studied like maximum spanning tree, minimum spanning tree etc. Among those the minimum spanning tree of a weighted graph is being inculcated in this paper for the implementation of the error control mechanism. Among all the possible spanning trees for a given connected, weighted graph, the tree with the minimum total weight is called as the Minimum Spanning Tree for that given graph. In order to determine the minimum spanning tree for any given graph, we can make use of any of the two algorithms, which are, Kruskal's algorithm and Prim's algorithm and among these two, Prim's algorithm has been incorporated in this paper. It is an algorithm in the graph theory using which the minimum spanning tree for any connected undirected weighted graph can be determined. It finds a subset of edges that covers all the vertices forming a tree where the total weight of all the edges in the tree is minimized.

The goal of this research is to develop and implement an algorithm in the field of error detection technique coupled with the traditional error correction methodologies. The paper elaborates on the problem being faced during transmission of data over a network subject to the correctness of the data being received in the Section (3), a brief explanation of the solution methodology/technique being introduced in the paper is given in the Section (4), the experiments and analysis performed during the research are explained with examples under Section (5) {(5.1), (5.2), (5.3), (5.4), (5.5)}, the end result is compiled in the Section (6) and final conclusion which is being derived from the paper is expressed in the Section (7).

2. Literature Review

Error correction and detection has formed a perennial application ground in various technical frame be it neural system, networking, transmission over a frequency channel, optical communication to just name a few.

This has led to many researchers to do a detailed probing in this field. Some of the research papers used as a reference for this paper work includes a new method based on the Reed Muller matrix which emphasizes over minimizing the amount of redundancy while maximizing the number of errors that can be corrected [1], help designers easily detect the error before the extraction process in 2D drawing[2],[3]. Maintaining a self-stabilizing spanning tree in a distributed system with few modifications the algorithm is being made more flexible and scalable by allowing nodes to join and leave the system whenever it wants to. Also application specific enhancements are suggested to the original algorithm which will make the algorithm very useful in security scenarios [4].

Another paper proposes a dynamic voltage scaling (DVS) technique, which inculcates an in-situ error detection and mechanism, called Razor [5], the minimal spanning tree being used for the study of cluster stability using two sampling distributions. The experiments explained in the paper demonstrate the ability of this approach towards the detection of the factual number of clusters [6]. Self-Stabilization by Local Checking and Correction [8].The main focus of this paper was on how the noise and multipath performance of the Frequency-Modulated Differential Chaos Shift Keying system can be improved by changing the transmitter and receiver configurations and also applies a non-redundant error correction to the detected error based on the minimum cost spanning tree algorithm. The use of graphs contributed to error correction and decision making at the receiver's end [11], Spanning tree approach in asynchronous network [12].

3. Detailed Problem Definition

The data transmission in the networking field is subjected to errors as these channels are not completely reliable. Thus error control techniques are being utilized in order to retain an error-free data at the receiver's end. In this research paper, the use of spanning tree approach is being made for the authentication of the data. The Prim's algorithm has been implemented in this paper and the minimum path generated using this approach is utilized for encoding the data at the sender's end and for error detection purpose at the receiver's end. This paper mainly emphasizes on the error detection part and the error correction is done by utilizing the traditional correction method which when coordinated with the proposed detection method using Prim's algorithm leads to a desired resultant data. For the implementation part of the algorithm, the high level language, that is, C is being used as programming tool in this paper.

4. Solution Methodology

4.1 The detection of the error achieved by implementing the Prim's algorithm.

The algorithm follows the following steps:

Step 1: Select and mark any vertex as a starting vertex.

Step 2: Find the next nearest neighbor of the selected vertex in step 1. Mark both the edges. Now mark the cheapest unmarked edge in the graph that doesn't form a close circuit.

Step 3: Find the nearest non traversed neighbor to the above formed sub graph. Mark it and the edge connecting the vertex to the sub graph.

Step 4: Repeat step 2 until all the vertices are traversed atleast once. Thus the sub graph so formed is a minimum spanning tree.

4.2 Architecture:

The above implementation follows the three basic levels of architecture, namely, User level, logical or conceptual level and the physical level as elaborated below:

4.2(a) Physical level: The user sends the data along with two files where in one file consists of the corresponding adjacency matrix of the undirected weighted graph. On the other hand the second file possesses the corresponding code for the retrieval/decoding of the meaningful sent data with respect to the minimum path being generated.

4.2(b) Logical level: The actual execution of the proposed algorithm, in this case the Prim's algorithm, embedded with new approach is implemented at this level. It interacts with the internal level for all data/ data file requirements.

4.2 (c) User level/external level: The final state of the implementation, that is, the checking of the correctness of the data is visualized in this level.

The figure 1.given below briefs about the architecture explained in the section (3.2).

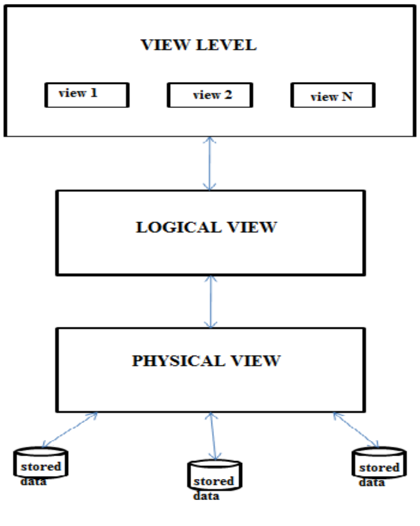


Figure. 1 Three basic levels of Architecture.

5. Details of the Analysis:

5.1 Error Detection using Prim's algorithm

Considering the following graph….

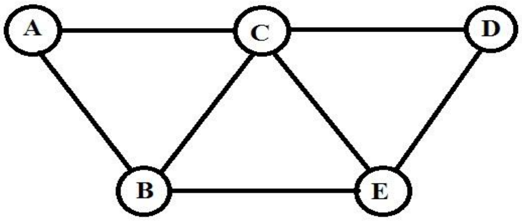


Figure. 2 Initial Connected Graph G.

The below GRAPH consists of set of nodes A,B,C,D,E which are connected in an undirected manner ,that is, if A is connected to B then B is also connected to A, along with their assigned weights. This forms the weighted undirected graph.

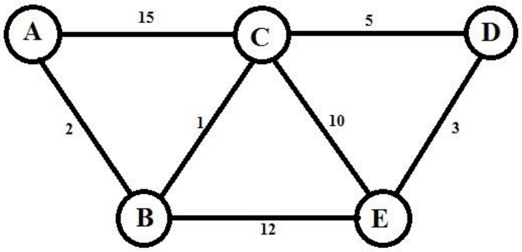


Figure. 3 Graph G with weight.

Now using the Prim’s Algorithm, the minimum spanning tree is generated such that it covers all the nodes in the given graph through the shortest path such that the sum of the weight of the edges is minimum. The resultant is called a tree as there are no loops or circles are eliminated.

5.2 How prim’s algorithm works:

1. Consider a starting node, say A.
2. Find the closest node in the tree which has a minimum weight, in the above case, its B.
3. Repeat the same procedure until all the n-1 edges are covered, where n is the number of nodes.

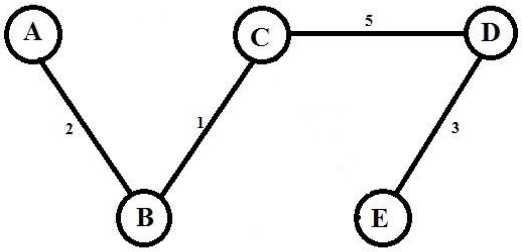


Figure. 4 Minimum Spanning tree for graph G.

The path being generated by the minimum spanning tree would be:

Starting node A

Node A→B

Node B→C

Node C→D

Node D→E

5.3 The proposed method of error detection in data being received based on the above algorithm…

Considering the following scenario that the user wants to send a data, for example say "HELLO"…

Step 1: All the alphabets forming the data, first has to be fed into an undirected graph that forms the vertices in such a manner that the assigning of weights are so done that it follows an increasing order and the correct sequence of data is maintained.

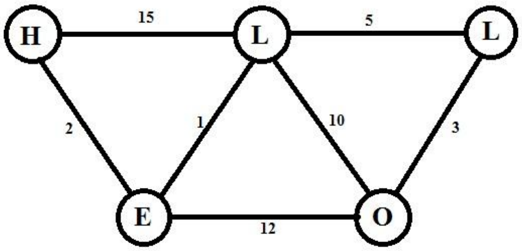


Figure. 5 Weighted Graph with data units.

Step 2: In the next step, Prim's algorithm is applied to generate the minimum spanning tree along the shortest path covering all the nodes of the initial graph such that the meaningful data is obtained.

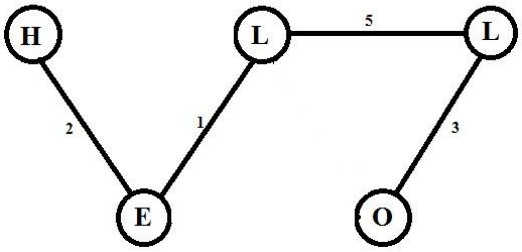


Figure. 6 Minimal Spanning Tree.

Step 3: The vertices containing the data along the shortest minimum path will generate the meaningful data as follows:

Starting node A ______ H

Node A→B ______ E

Node B→C ______ L

Node C→D ______ L

Node D→E ______ O

Adjacency Matrix: The adjacency matrix for the above example graph with five nodes is given below where the order of the matrix is (n X n) {n: number of vertices}

$$\begin{array}{c|ccccc|}
 & A & B & C & D & E \\
A & 0 & 2 & 15 & 0 & 0 \\
B & 2 & 0 & 1 & 0 & 12 \\
C & 15 & 1 & 0 & 5 & 10 \\
D & 0 & 0 & 5 & 0 & 3 \\
E & 0 & 12 & 10 & 3 & 0
\end{array}$$

5.4 Conclusion of the Analysis:

For the correctness of the sequence of the data, we have to compare the received data and the data being formed by decoding the shortest path being generated by using the Prim's algorithm. After the comparison if both the data are equivalent, then we can say that the data being received at the receiver's end is error-free. If this comparison evaluates to be false then there is error in the received data.

5.5 Error Correction

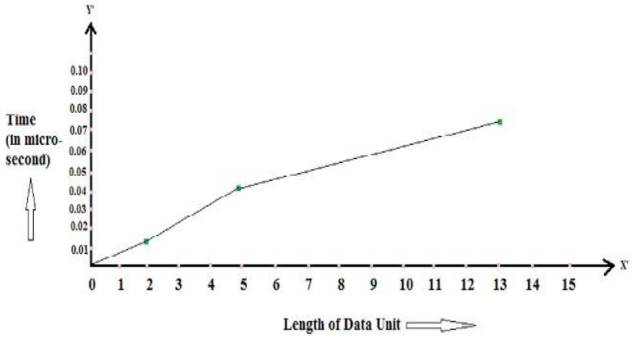
The data which is being encountered with error is then passed through the error correction process. It is a mechanism using which changes can be made in the received erroneous data in order to get an error free data.

There are two very common error correction techniques which are employed, namely, error correction by retransmission and forward error correction. The proposed method for detection of error can be implied with any of the traditional correction methodology

6. Results

The approximation of the time complexity of the proposed method is equivalent to the Prim's algorithm, that is of the order O(n^2) and comparatively it works effectively on small data units.

Given below is a graph analysis showing the time complexity for three sample data units of varying length:



Time Complexity Graph on 3 sample data units

7. Conclusion and Future Enhancement

The paper can be concluded with the positive result that the proposed method incorporated with the Prim's algorithm, in the error control technique is providing the desired output subject to small data unit. For future enhancement we can implement the proposed method with some new ideas on large data units.

References:

1. Khalid Faraj , "Design Error Detection and Correction System based on Reed_Muller Matrix for Memory Protection", Birzeit University Department of Computer Systems Engineering Birzeit, International Journal of Computer Applications (0975 – 8887) Volume 34– No.8, November 2011 42
2. MohdShafryMohd Rahim, AmjadRehman, Mohamad Faizal Ab Jabal, TanzilaSaba, "Close Spanning Tree (Cst) Approach For Error Detection And Correction For 2d Cad Drawing", Graphics and Multimedia Department, Faculty of Computer Science and Information Systems UniversitiTechnologi (Malaysia),International Journal of Academic Research Vol. 3. No.4 July, 2011, II Part
3. Mohamad Faizal Ab Jabal, MohdShafryMohd Rahim, MohdDaudKasmuni, Daut Daman, AmjadRehman and TanzilaSaba," Close Spanning Tree (CST) Approach for Error Detection and Correction for 2D CAD Drawing", Journal of Computing, Volume 2, Issue 8, August 2010, ISSN 2151-9617
4. BharathBalasuaramanian, MeghnaDeodhar, "Performance Evaluation and Analysis of a Self=Stabilizing Spanning Tree Algorithm," Distributed Systems, EE382N
5. Shidhartha Das, David Roberts, Seokwoo Lee, Sanjay Pant,David Blaauw, Member, Todd Austin, KrisztiánFlautner, Member, and Trevor Mudge, "A Self-Tuning DVS Processor using Delay-Error Detection and Correction", IEEE Journal of solid-state circuits, vol. 41, no. 4, April 2006

6. ZeevBarzily, ZeevVolkovich, BasakAkteke-Öztürk and Gerhard-Wilhelm Weber, "On A Minimal Spanning Tree Approach In The Cluster Validation Problem," ORT Braude College of Engineering, Institute of Applied Mathematics, Middle East Technical University
7. Alex Gorod, Ryan Gove, Brian Sauser, John Boardman, "System of Systems Management: A Network Management Approach," Charles V. Schaefer, Jr. School of Engineering Stevens Institute of Technology Castle Point on Hudson
8. Baruch Awerbuch, Boaz Patt-Shamirt, George Vargheset, "Self-Stabilization By Local Checking and Correction extended abstract," Laboratory for Computer Science Massachusetts Institute of Technology
9. Jana van Greunen, Jan Rabaey, "Lightweight Time Synchronization for Sensor Networks", University of California, Berkeley
10. Nicholas E. Matsakis, "Recognition of Handwritten Mathematical Expressions," Submitted to the Department of Electrical Engineering and Computer Science in partial fulfilment of the requirements for the degrees of Bachelor of Science in Electrical Engineering and Computer Science and Master of Engineering in Electrical Engineering and Computer Science at the Massachusetts Institute of Technology
11. Zolt´anJ´ak´o Daniele Fournier-Prunarety Veronique Guglielmiy and G´aborKis, "Non-Redundant Error Correction in FM-DCSK," ECCTD'01 - European Conference on Circuit Theory and Design, August 28-31, 2001
12. Sudhanshu Madan Aggarwal, "Time optimal Self-Stabilizing Spanning Tree Algorithms,"Massachusetts Institute of Technology, May 1994
13. Shay Kutten, "Scalable Fault Tolerance," Faculty of Industrial Engineering, Technion , Hafia 32000, Israel, and IBM T.J
14. K. Suresh, K.Venkataramana, "Study of analysis on RSA and its variants" in International Journal of Computer Science Research & Technology, vol. 1, issue 4, 2013
15. RohitMinni, Kaushal Sultania, Saurabh Mishra, Durai Raj Vincent, "Enhancing security features in RSA cryptosystem" in Computing, Communications and Networking Technologies, 2013.
16. C.C. Chang and M.S. Hwang "Parallel computation of the generating keys for RSA cyptosystems". IEEE 1996
17. Mayank Jhalani, Piyush Singh, Gaurav Shrivastava, "Enhancement over the variant of public key cryptography algorithm," in International journal of emerging technology and advanced engineering, Vol. 2, Issue 12, Dec. 2012

18. NavaneetOjha, SahadeoPadhye "Cryptanalysis of multi prime RSA with secret key greater than public key," International Journal of network security, vol.16, no.1, pp.53-57, Jan. 2014

19. Hung-min sun, Mu-enwu, Wei-chi ting, and M. Jason Hinek "Dual RSA and its security analysis," IEEE transactions on information theory, vol. 53, no. 8, august 2007.

20. B R Ambedkar& S SBedi, "A New Factorization Method to Factorize RSA Public Key Encryption", IJCSI International Journal of Computer Science Issues, Vol. 8, November 2011.

21. Chhabra A, Mathur S., 2011, "Modified RSA algorithm: a secure approach". In: International Conference on Computational Intelligence and Communication Networks, Gwalior; 2011.

22. Forouzan BA.2007, "Cryptography and network security". Special Indian Edition. Tata McGraw-Hill, p. 2011.

23. Ali H, Salami MA. 2004, "Timing attack prospect for RSA cryptanalysts using genetic algorithm technique". Int Arab J InfTechnol 2004.

24. Rivest RL, Shamir A, Adleman LA.1978, "Method for obtaining digital signatures and public-key cryptosystems". Commun ACM.

25. Hung-min sun, mu-enwu, wei-chi ting, and m. jasonhinek "Dual RSA and its security analysis". IEEE transactions on information theory, vol. 53, no. 8, august 2007.

26. Ximeng Liu, Jianfeng Ma, JinboXiong, Qi Li, Tao Zhang, Hui Zhul "Threshold attribute-based encryption with attribute hierarchy for lattices in the standard model"-IET 2013

27. Thangavel, M., P. Varalakshmi, MukundMurrali, K. Nithya, "An Enhanced and Secured RSA Key Generation Scheme (ESRKGS)," in Journal of information Security and application, Vol. 20, 2015, pp. 3-10.

28. Ravi Shankar Dhakar, Amit Kumar Gupta, Prashant Sharma, 2012," Modified RSA Encryption Algorithm (MREA)" advance Advanced Computing & Communication Technologies (ACCT).

29. Chandrasegar Thirumalai, Senthilkumar M, "An Assessment Framework of Intuitionistic Fuzzy Network for C2B Decision Making", International Conference on Electronics and Communication Systems (ICECS), 2016

30. Vaishnavi B, Karthikeyan J, Kiran Yarrakula, Chandrasegar Thirumalai, "An Assessment Framework for Precipitation Decision Making Using AHP", International Conference on Electronics and Communication Systems (ICECS), 2016

31. M.Senthilkumar, T.Chandrasegar, M.K. Nallakaruppan, S.Prasanna, "A Modified and Efficient Genetic Algorithm to Address a Travelling Salesman Problem," in International Journal of Applied Engineering Research, Vol. 9 No. 10, 2014, pp. 1279-1288

32. Vinothini S, Chandra Segar Thirumalai,,Vijayaragavan R, Senthil Kumar M, "A Cubic based Set Associative Cache encoded mapping International Research Journal of Engineering and Technology (IRJET)," Volume: 02 Issue: 02 May -2015

33. T Chandra Segar, R Vijayaragavan, "Pell's RSA key generation and its security analysis," in Computing, Communications and Networking Technologies (ICCCNT) 2013, pp. 1-5.

34. Chandramowliswaran N, Srinivasan.S and Chandra Segar.T, "A Novel scheme for Secured Associative Mapping" The International J. of Computer Science and Applications (TIJCSA) & India, TIJCSA Publishers & 2278-1080, Vol. 1, No 5 / pp. 1-7 / July 2012

35. Chandramowliswaran N, Srinivasan.S and Chandra Segar.T, "A Note on Linear based Set Associative Cache address System" International J. on Computer Science and Engg. (IJCSE) & India, Engineering Journals & 0975-3397, Vol. 4 No. 08 / pp. 1383-1386 / Aug. 2012.

36. Bellini, Emanuele, and Nadir Murru. 2015. "An Efficient and Secure RSA--like Cryptosystem Exploiting R'edei Rational Functions over Conics." : 1–18. http://arxiv.org/abs/1511.03451.

37. "DDoS: Survey OfTraceback Methods", International Joint Journal Conference in Engineering 2009, ISSN 1797-9617.

38. "Anti-Piracy For Movies Using Forensic Water Marking", in IJCA Digital Library on February 15, 2013, ISBN: 973-93-80872-84-0.

39. A Novel Interpolation Based Super Resolution of the Cropped Scene from a Video" Published in IJERT on March 2013, ISSN:2278-0181.

40. Uncertain Data Prediction on Dynamic Road Network, IEEE ICICES 2014.

41. Various Indexing and query processing Techniques in spatio-temporal data, ICTACT Journal on Soft Computing (Volume: 6 , Issue: 3), April,2016.

42. M.K.NallakaruappanM.Senthilkumar, U.Senthilkumaran, "Review of asymmetric key cryptography in wireless sensor networks," International Journal of Engineering and Technology, Vol. 8 Issue 2 pp. 859-862, 2016

43. Dr.P.Ilango, M.Senthilkumar, “A Survey on Job Scheduling in Big Data,” in Journal of Cybernetics And Information Technologies, Vol. 16 Issue 3 pp. 35-51
44. P Viswanathan, P Venkata Krishna, “Text fusion watermarking in medical image with semi-reversible for secure transfer and authentication,” Advances in Recent Technologies in Communication and Computing, 2009. ARTCom'09. pp. 585-589
45. P Viswanathan, P Venkata Krishna, “A Joint FED Watermarking System Using Spatial Fusion for Verifying the Security Issues of Teleradiology,” IEEE Journal of Biomedical and Health Informatics, Vol.8, Issue 3, pp.753-764
46. P Viswanathan, “Fusion of cryptographic watermarking medical image system with reversible property,” in Computer Networks and Intelligent Computing 2011 pp.533-540.
47. Chandrasegar Thirumalai, Senthilkumar M, Vaishnavi B, “Physicians Medicament using Linear Public Key Crypto System,” in International conference on Electrical, Electronics, and Optimization Techniques IEEE-ICEEOT, March 2016.
48. Ellen Jochemsz, and Benne de Weger, “A Partial Key Exposure Attack on RSA using a 2-Dimensional Lattice,” LNCS, Information Security, 2006, Vol. 4176, pp.203-216
49. P Viswanathan, P Venkata Krishna, S Hariharan, “Multimodal Biometric Invariant Moment Fusion Authentication System,” in Information Processing and Management 2010, pp. 136-143
50. Chandramowliswaran, N., S. Srinivasan, and P. Muralikrishna. "Authenticated key distribution using given set of primes for secret sharing," Systems Science & Control Engineering 2015, Vol.3, Issue 1, pp. 106-112.
51. Chandrasegar Thirumalai, “Physicians Drug encoding system using an Efficient and Secured Linear Public Key Cryptosystem (ESLPKC),” Vol. 8 Issue 3, Sep. 2016 pp. 16296-16303.