Global Journal of Engineering and Technology [GJET].
ISSN: **2583-3359** (Online)
Frequency: Monthly
Published By GSAR Publishers
Journal Homepage Link- https://gsarpublishers.com/journal-gjet-home/

A STUDY OF MESSAGE ENCRYPTION THROUGH WHATSAPP USING GRAPH LABELING

BY

Sreena T D
Assistant Professor Department of Mathematics Sree Narayana College Nattika, Thrissur, Kerala.

Article History

Received: 03/02/2024
Accepted: 17/02/2024
Published: 20/02/2024

Vol – 3 Issue – 2

PP: - 37-38

Abstract:
This paper means to examine the transmission of messages through WhatsApp network and investigates the degree to which the messages are transmitted. I likewise attempt to foster a calculation to distinguish the senders of the specific message through that network. I attempt to associate graph labeling with these networks for the examination of the information.

Keywords: *Communication, Encryption, Labeling, Message, Network*

1. INTRODUCTION

WhatsApp Messenger is an American freeware, get stage unified informing and voice-over-IP administration claimed by Facebook, Inc. It permits clients to send instant messages and voice messages, settle on voice and video decisions, and offer pictures, archives, client areas, and other substance.

WhatsApp's start-to-finish encryption is utilized when you message someone else utilizing WhatsApp Messenger. Start-to-finish encryption guarantees just you and the individual you're speaking with can peruse or tune in to what exactly is sent, and no one in the middle, not even WhatsApp.

End-to-end encryption is the most secure approach to convey secretly and safely on the web. By scrambling messages at the two closures of a discussion, start-to-finish encryption keeps anybody in the center from perusing private correspondences. This varies from the encryption that most organizations as of now use, which just secures the information on the way between your gadget and the organization's workers. For instance, when you send and get an email utilizing an assistance that doesn't give E2EE, like Gmail or Hotmail, the organization can get to the substance of your messages since they additionally hold the encryption keys. E2EE kills this chance on the grounds that the specialist organization doesn't really have the decoding key. Along these lines, E2EE is a lot more grounded than standard encryption.

WhatsApp characterizes end-to-end encryption as correspondences that remain scrambled from a gadget constrained by the sender to one constrained by the beneficiary, where no outsiders, not even WhatsApp or our parent organization Facebook, can get to the substance in the middle. An outsider in this specific situation implies any association that isn't the sender or beneficiary client straightforwardly taking an interest in the discussion.

By graph labeling we mean the assignment of weights to nodes or arcs or to both. Various sorts of labelings had been characterized till date and different uses of labelings were additionally contemplated in [4]. In [1] and [2], A.Nagoor Gani and D.Rajalaxmi (a) subahashini, have defined and explained properties of fuzzy labeling.

In this paper, I attempt to apply graph labeling for network examination so that labelings can be utilized for distinguishing the senders of a specific message.

2. PRELIMINARIES

Definition 2.1 A graph G = (σ, μ) is a fuzzy labeling graph if there exist two bijective functions σ:V→[0,1] and $\mu : E \rightarrow$ [0,1] such that $\mu(u,v) < \sigma(u) \wedge \sigma(v)$ for all u, v in V.

Definition 2.2 An acyclic directed graph is said to be a directed tree.

Definition 2.3 A tree with an ordering at each level is called an ordered tree.

3. MAIN RESULTS

Definition 3.1 (Fuzzy pseudo Labeling)
A graph G = (σ, μ) is a fuzzy pseudo labeling graph if there exist two functions σ:V→[0,1] and $\mu : E \rightarrow$[0,1] such that $\mu(u,v) < \sigma(u) \wedge \sigma(v)$ for all u, v in V. A graph with fuzzy pseudo labeling is called a fuzzy pseudo labeled graph, and a

*Corresponding Author: Sreena T D

directed graph with fuzzy pseudo labeling is said to be a fuzzy pseudo labeled digraph.

Example 3.2

Consider G = (V, E) where V = {u, v, w, x}.

Define: V → [0,1] by σ (u) = $\frac{1}{4}$, σ (v) = $\frac{1}{4}$, σ (w) = $\frac{3}{4}$, σ (x) = 1 and

$\mu : E \rightarrow$ [0,1] by $\mu(v_i, v_j) = \sigma(v_i) \cdot \sigma(v_j)$.

Then $\mu(u, v) = \frac{1}{16}$, $(u, w) = \frac{3}{16}$, $\mu(u, x) = \frac{1}{4}$ and $\mu(v, w) = \frac{3}{16}$.

Hence G is a fuzzy pseudo-labeled graph.

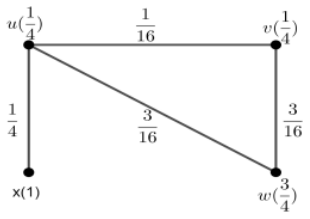

Fig. 1

Definition 3.3

Let DT = (V, E) be a directed ordered tree with the node set V = (v_1,v_2,…,v_n) and a set E of arcs. Then DT is said to have message labeling if there exist two functions σ and μ such that σ : V → [0,1] defined by $\sigma(v_i)=(\sigma_1(v_i), \sigma_2(v_i))$,where $\sigma_1(v_i)$ = $\frac{Number\ of\ children\ of\ v_i}{Total\ numbers\ of\ nodes\ in\ the\ next\ level}$ and $\sigma_2(v_i)$ = $\frac{Number\ of\ ancestors\ of\ v_i}{Total\ numbers\ of\ nodes}$.

Also $\mu : E \rightarrow$ [0,1] defined by $\mu(v_i, v_j) = (\mu_1(v_i, v_j), \mu_2(v_i, v_j))$, where $\mu_1(v_i, v_j) = \sigma_1(v_i)\sigma_1(v_j)$ and $\mu_2(v_i, v_j) = \sigma_2(v_i)\sigma_2(v_j)$.The graph which admits message labeling is called a message labeling graph.

Remark 3.4

Message labeling is a fuzzy pseudo digraph labeling.

4. ANALYSIS

The starting point of the network of a message is the sender of that specific message. As the message is sent from the starting point, it reaches at distinctive individual/persons. That recipient may disregard the message or send the message to other people. This interaction proceeds in various stages. However, the issue emerges when a few group send deluding/destructive message to the general public or even to the country. At that point, these network ought to be investigated altogether to keep away from the threaten.

Despite the fact that it is an E2EE, there might be a few cases which needs interruption of the security office or the public authority. Define the network as a rooted directed ordered tree with the root node as the starting point. The desecedants of the tree are the recipients of that specific message. The leafs of the tree are the recipients who are not sending the messages. The children of a node is the number of recipients of the message from that particular node.

By making message labeling as a tool for analysing the message transmission, the node with degree (1,$\frac{n-1}{n}$), where n is the number of nodes - is the root of that message, and the path in the tree whose sum of degrees is higher is the channel through which the message is transmitted in a suspicious manner.

Hence in the communication network, the problem aims to maximize the function $\sum_{u,v} \rho(u, v)$ subject to the constraints $\rho(u, v) \geq 0, \mu(u) \geq 0,$ $\mu(u_0) = 1$ and $and\ \mu(v_n) = 1,$ where u_0 is the root and v_n is the leaf. The root with maximum $\sum_{u,v} \rho(u, v)$ is named as the suspected node , the corresponding person in the network is the suspected person.

5. CONCLUSION

In this paper, I dissected the transmission of a message through WhatsApp and discover an instrument to perceive the origin of that message and the channel through which it is generally conveyed. I trust this can be utilized in communication network for the examination of informations. I also identified that the problem reduces to an optimization problem subject to certain conditions which leads to more research in that area.

REFERENCES

1. A. Nagoor Gani and D. Rajalaxmi (a) Subahashini, "*A note on fuzzy labeling*", International Journal of Fuzzy Mathematical Archive, Vol. 4, No. 2, 2014, 88-95.
2. A.Nagoor Gani and D.Rajalaxmi (a) Subahashini, "*Properties of fuzzy labeling graph*", Applied Mathematical Sciences, January 2012.
3. "*WhatsApp encryption Overview*", Technical White Paper, October 22, 2020.
4. Joseph A Gallian, "*A dynamic survey of graph labeling*", The Electronic Journal of Combinatorics, December 2020.
5. Henniges, U., Prohaska, T., Banik, G., & Potthast, A. (2006). A fluorescence labeling approach to assess the deterioration state of aged papers. *Cellulose*, *13*, 421-428.
6. Beel, J., Langer, S., & Genzmehr, M. (2013). Sponsored vs. organic (research paper) recommendations and the impact of labeling. In *Research and Advanced Technology for Digital Libraries: International Conference on Theory and Practice of Digital Libraries, TPDL 2013, Valletta, Malta, September 22-26, 2013. Proceedings 3* (pp. 391-395). Springer Berlin Heidelberg.

*Corresponding Author: Sreena T D