



Totally Antimagic Total Labelling of a Complete Bipartite Graph and its Application in End-to-End Encryption

Ode Jane¹, Atu Myom²

¹Department of Maths/Computer Sc. Benue State University Makurdi, Nigeria

²WAPTEG Technologies, Makurdi Benue State Nigeria

Abstract: One of the major challenges facing end-to-end encryption is that of Man-in-the-Middle attacks; End-to-end encryption ensures that data is transferred securely between endpoints. But, rather than try to break the encryption, an eavesdropper may impersonate a message recipient (during key exchange or by substituting his public key for the recipient's), in an attempt to combat this challenge we modelled a dynamic encryption with implicit key exchange for end-to-end encryption using the concept of graph theory, by applying TAT labelling over the network we will eliminate explicit key i.e. during transmission; keys will be computed implicitly using parameters over the graph network and the end receiver will not need to exchange any key thereby making it impossible to successfully intercept the message as it can only be extracted at the intending source.

Keywords: Totally Antimagic Total Labelling; End-To-End Encryption; Bipartite Graph; Network; Labelling

I. Introduction

Graph labeling is the assignment of integers to the vertices or edges, or both subject to certain conditions. Graph labeling was first introduced in the mid 1960's, most of the graph labeling methods trace their origin to the one introduced by Rosa in 1967 or one given by Graham and Sloane [1]. In the subsequent four decades well over 1000 papers on graph labeling have been studied. There are many types of graph labeling, but this work is restricted to TAT labeling. [2] introduced the concept of TAT labeling. For a graph G , a bijection from the vertex set and the edge set of G to the set $\{1, 2, 3, \dots, |V(G)| + |E(G)|\}$ is called a total labeling of G . A total labeling is called edge-antimagic total or vertex-antimagic total if all the edge weights or vertex weights are pairwise distinct. If a labeling is simultaneously edge-antimagic total and vertex-antimagic total, it is called a totally antimagic total labeling [2].

This study utilizes TAT labeling of a complete bipartite graph for a dynamic key generation of end-to-end encryption. **End-to-end encryption (E2EE)** is a system of communication where only the communicating users can read the messages. In principle, it prevents potential eavesdroppers – including telecom providers, Internet providers, and even the provider of the communication service – from being able to access the cryptographic keys needed to decrypt the conversation [6]. The systems are designed to defeat any attempts at surveillance or tampering because no third parties can decipher the data being communicated or stored. For example, companies that use end-to-end encryption are unable to hand over texts of their customers' messages to the authorities.

In an E2EE system, encryption keys must only be known to the communicating parties. To achieve this goal, E2EE systems can encrypt data using a pre-arranged string of symbols, called a pre-shared secret, or a one-time secret derived from such a pre-shared secret. They can also negotiate a secret key on the spot using Diffie-Hellman key exchange.

As of 2016, typical server-based communications systems do not include end-to-end encryption. These systems can only guarantee the protection of communications between clients and servers, meaning that users have to trust the third-parties who are running the servers with the original texts [7].

One of the major challenges facing end-to-end encryption is that of Man-in-the-Middle attacks; End-to-end encryption ensures that data is transferred securely between endpoints. But, rather than try to break the encryption, an eavesdropper may impersonate a message recipient (during key exchange or by substituting his public key for the recipient's), so that messages are encrypted with a key known to the attacker. After decrypting the message, the snoop can then encrypt it with a key that he or she shares with the actual recipient, or his or her public key in case of asymmetric systems, and send the message on again to avoid detection. This is known as a man-in-the-middle attack.

In an attempt to combat this challenge we are proposing a dynamic encryption without key exchange for end-to-end encryption using the concept of graph theory. One way an eavesdropper can lay hold on a sender or receiver's key is by invading his device and extract the key or during key exchange. By applying TAT labeling over the network we will eliminate explicit key exchange and no user will have a key, i.e. during transmission; keys will be computed implicitly using parameters over the graph network and the end receiver will not need to exchange any key, the key will be computed using his node over the graph network. In this way once there's an attempt to intercept on the network, the interceptor automatically receives a label which makes it impossible to decrypt the transmission. The encryption is designed to decrypt only at the destination points because only the destination node has the right combination over the network label to decrypt. The network labeling is reassigned periodically to strengthen the security policy.

II. Related Works

Graph labeling is used in many applications like coding theory, x-ray crystallography, radar, astronomy, circuit design, communication, network addressing and data base management. [5] Showed how to achieve high level of security by using magic squares of order 16. [3] Explored the role of labeling in expanding the utility of channel assignment process in communication networks and addressed how the concept of graph labeling can be applied in network security. [5] Used vertex magic total labeling of complete graphs to provide add on security to existing ASCII based cryptosystem, their method strengthens the encryption process by considering a large matrix base for key generation. Their research focuses more on preventing encryption key guessing however, in the situation where there is a stolen key this method will be limited.

III. Methods

In this research work, we will be using TAT labelling over a closed network (intranet) to improve on an end-to-end encryption.

A. TAT Labeling Model

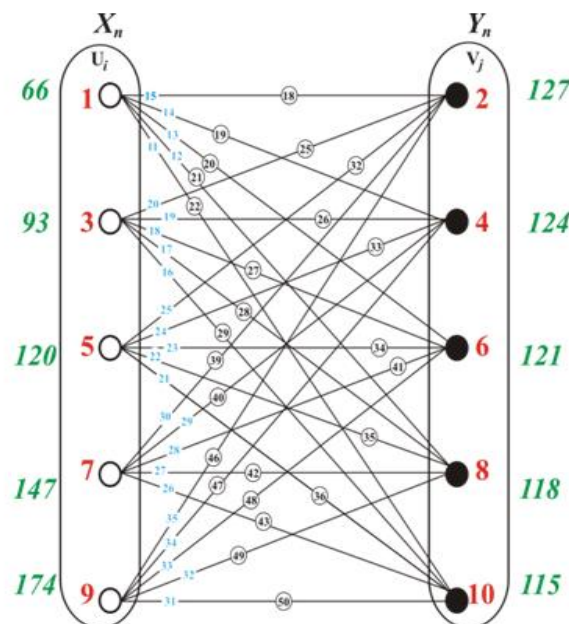


Figure 1: TAT Labeling Model of a $K_{5,5}$ Graph

From figure 1 transmission is carried out between connecting vertexes for example when transmitting between U_1 and V_2 the following parameters will be considered u_1 vertex label= a , v_2 vertex label= b , file size= c , expected delivery time= d , u_1 weights= e , v_2 weight= f . using this parameters we will encrypt the transmission such that only the receiving vertex or node will have the sufficient implicit information to decrypt. This method completely eliminates man-in-the-middle attack because the moment you intercept on the network you will be assigned unique vertex properties which are of course different from the intended destination thereby leaving you with limited information to be able to decrypt.

In generating the label model consider the equation

Lemma: Let $n > 3 \in \mathbb{Z}^+$, then the graph $K_{n,n}$ is a super totally antimagic total graph.

Proof:

The graph $K_{n,n}$ is partitioned into two equal sets X_n and Y_n

The vertices of X_n are denoted by the symbols

$u_i, i = 1, 2, \dots, n, u_i \in X_n$

and vertices of Y_n by the symbols,

$$v_j, j = 1, 2, \dots, n, v_j \in Y_n$$

The labeling f for the graph $K_{n,n}$ is defined by;

$$f: V(K_{n,n}) \cup E(K_{n,n}) \rightarrow \{1, 2, \dots, p + q\}$$

Where p and q represent the total number of elements in the vertex set and edge set respectively.

Hence, the labeling of the graph $K_{n,n}$, is defined in the following way;

$$f(u_i) = 2i - 1 \quad (1)$$

where $f(u_i)$ is the labeling of the vertices in the set X_n .

$$f(v_j) = 2j \quad (2)$$

Where $f(v_j)$ is the labeling of the vertices in the set Y_n

$$f(u_i v_j) = n(2 + i) - (j - 1), \quad i, j = 1, 2, \dots, n, \quad (3)$$

Where $f(u_i v_j)$ is the labeling of all the edges.

It is deduced from equation 1 and 2 that the graph $K_{n,n}$ is super.

The edge-weights under the labeling f are given by;

$$\begin{aligned} wt_f(u_i v_j) &= f(u_i) + f(u_i v_j) + f(v_j) \\ &= 2i - 1 + n(2 + i) - (j - 1) + 2j \end{aligned} \quad (4)$$

The vertex weights for the vertices, $u_i \in X_n$ under the labeling f are given by;

$$\begin{aligned} wt_f(u_i) &= f(u_i) + \sum_{j=1}^n f(u_i v_j), \quad i, j = 1, 2, \dots, n \\ &= 2i - 1 + \sum_{j=1}^n n(2 + i) - (j - 1) \\ &= i(2 + n^2) + \frac{n}{2}(1 + 3n) - 1 \end{aligned} \quad (5)$$

The above weights are pair wise distinct which implies that the labeling is an EAT labeling.

The vertex weights for the vertices, $v_j \in Y_n$ under the labeling f , are given by;

$$\begin{aligned} wt_f(v_j) &= f(v_j) + \sum_{i=1}^n f(u_i v_j), \quad i, j = 1, 2, \dots, n \\ &= 2j + \sum_{i=1}^n n(2 + i) - (j - 1) \\ &= j(2 - n) + \frac{n^2}{2}(5 + n) + n \end{aligned} \quad (6)$$

B. Architecture

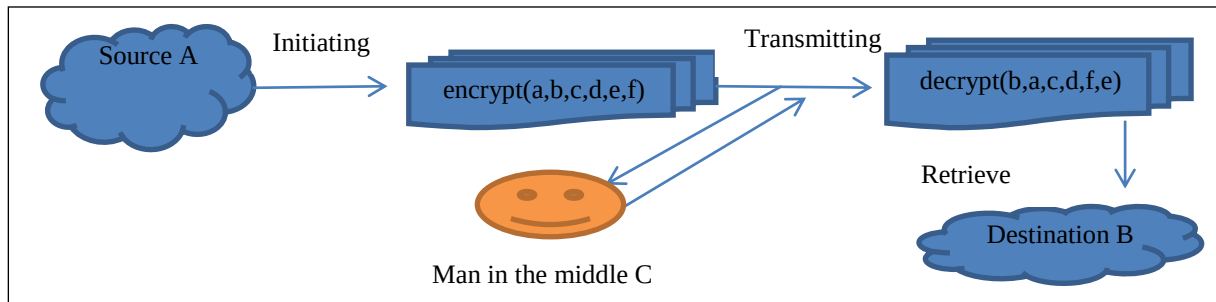


Figure 2: System Architecture

IV. Results and Discussions

From our model in Figure 1 we have the following transmission channels as show in Table I below

Table I Showing some of the Communication Channels.

Transmission	Transmission		
	Source	Path	Destination
1	U1	V1,U2	V2
2	U3	U3,V4	V4
3	U5	U5,V6	V6
4	U7	U7,V8	V8
5	U9	U9,V10	V10
6	U1	U1,U4	U4
7	U1	{1,U3},{6,U3}	U3
8	V2	{1,V4},{11,V4}	V4
9	V4	{12,V10}	V10
10	U3	{13,U9}	U9
11	V2	V2,U3	U3
12	V4	V4,U9	U9
13	U3	U3,V10	V10

From our results as in Table 1 is showing some transmission channels, we have direct transmission channels such as channels 1-6 and 11-13. These channels implements a single layer encryption security policy even as the risk of attack here is relatively low, as transmission is fast it does not give enough room for the attackers to initiates their process without been suspected; this is not to say security here could easily be compromised as decryption can only be successful at the intended destination. As transmission process becomes complex our model begins to implement multi-layer encryption as seen in 9; data is first moved on encrypted transmission 12 then further encrypt to destination V10. To further throw attackers off balance most communication channels have alternative transmission paths as in 6 and 7. The system is designed to choose any of the alternative paths to transmit.

References

- [1] J. Gallian, A dynamic survey of graph labeling, *Electronic Journal of Combinatorics*, vol. 14, 2013.
- [2] M. Baca., M. Miller, O. Phanalasy, J. Ryan , S.F. Andrea and A.A. Sillasen, Totally antimagic total graphs. *Australian Journal of combinatorics*, Vol 61, Issue , 2015, pp.42-56.
- [3] N. Prasanna. and K. Sravanthi, Application of Graph Labelling in Communication Networks, *Oriental Journal of Science and Technology*, 2014.
- [4] H. Krishnappa, N. Srinath, and S. Manjunath, Vertex Magic Total Labeling of Complete Graphs and their Applications for Public Key Cryptosystem, *International Journal of Innovative Research in Computer and Communiation Engineering*, vol **1**, **issue 2**, 2013, pp.379-387.
- [5] G. Gopinanth and K. Mani, Add-on Security Model for Public-Key Cryptosystem Based on Magic Square Implementation, *Proceedings of the world congress on Engineering and Computer science*, vol 1 WCECS 2009, October 20-22, 2009, San Francisco, USA.
- [6] *Hacker Lexicon: What Is End-to-End Encryption?"*. *WIRED*. Retrieved 22 December 2015<https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption>
- [7] *End-to-End Encryption. EFF Surveillance Self-Defence Guide. Electronic Frontier Foundation*. Retrieved 2 February 2016. <https://ssd.eff.org/en/glossary/end-end-encryption>