Journal of Informatics and Mathematical Sciences
Vol. 9, No. 3, pp. 949–955, 2017
ISSN 0975-5748 (online); 0974-875X (print)
Published by RGN Publications

http://www.rgnpublications.com

Proceedings of the Conference
Current Scenario in Pure and Applied Mathematics
December 22-23, 2016
Kongunadu Arts and Science College (Autonomous)
Coimbatore, Tamil Nadu, India

Research Article

A New Encryption Technique Using Detour Metric Dimension

V. Kala Devi[1] and K. Marimuthu[2,*]

[1] *Department of Mathematics, Bishop Heber College, Trichy 620 017, Tamilnadu, India*
[2] *Department of Mathematics, Ramco Institute of Technology, Rajapalayam 626117, Tamilnadu, India*
***Corresponding author:** marismphil@gmail.com

Abstract. A set of vertices W' detour resolves a graph G if every vertex is uniquely determined by its vector of detour distances to the vertices in W'. A detour metric dimension of G is the minimum cardinality of a detour resolving set of G. In this paper, detour metric dimension of certain graphs are investigated by detour distance matrix.

Keywords. Detour resolving set; Detour metric dimension; Encryption and Decryption

MSC. 05C12; 05C90

Received: December 29, 2016 **Accepted:** March 10, 2017

1. Introduction

All graphs considered here are simple, finite and connected. Let $G = (V,E)$ be a graph with V as the vertex set and E as the edge set. Let $u,v \in V$. The distance $D(u,v)$ is the length of the longest $u-v$ path in G. Let $W' = \{w_1,w_2,\dots,w_p\}$ be an ordered subset of V. For every $v \in V$, a representation of v with respect to $W'$is defined as p tuples, $R(v|W') = (D(v,w_1), D(v,w_2), \ldots, D(v,w_p))$. The set W' is a *detour resolving set* of G if every two distinct vertices $u,v \in V$ satisfy $R(u|W') \neq R(v|W')$. A *detour basis* of G is a detour resolving set of G with minimum cardinalityand the *detour metric dimension* of G refers to its cardinality, denoted by $D\beta(G)$.

The metric dimension [1–3] in general graphs was firstly studied by Harary and Melter [4], and independently by Slater [11, 12]. However, we have been obtained the relation between metric dimension and detour metric dimension for certain class of graphs, such as cycles, wheels, regular k-bipartite graphs, Cartesian product graphs [9] and etc. The purpose of this paper is to further investigate the detour metric dimension of certain graphs by detour distance matrix [5–8, 10].

2. Detour Metric Dimension for Some Standard Graphs

Theorem 2.1. *For the Jahangir graph $J_{2,m}$, $m \geq 3$, $D\beta(J_{2,m}) = 2m-1$.*

Proof. Let $V(J_{2,m}) = \{u_i/1 \leq i \leq 2m+1\}$ and

$$E(J_{2,m}) = \{u_i u_{i+1}/1 \leq i \leq 2m-1\} \cup \{u_i u_{2m+1}/i = 1,3,5,\ldots,2m-1\} \cup \{u_{2m}u_1\}$$

be the vertex set and edge set of the Jahangir graph $J_{2,m}$, $m \geq 3$.

The Detour Distance Matrix of $J_{2,m}$ is given in Figure 1.

	u_1	u_2	u_3	u_4	$\ldots$	u_{2m}	u_{2m+1}
u_1	0	$2m-1$	$2m-2$	$2m-1$	$\ldots$	$2m-1$	$2m-1$
u_2	$2m-1$	0	$2m-1$	$2m$	$\ldots$	$2m$	$2m$
u_3	$2m-2$	$2m-1$	0	$2m-1$	$\ldots$	$2m-1$	$2m-1$
u_4	$2m-1$	$2m$	$2m-1$	0	$\ldots$	$2m$	$2m$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
u_{2m}	$2m-1$	$2m$	$2m-1$	$2m$	$\ldots$	0	$2m$
u_{2m+1}	$2m-1$	$2m$	$2m-1$	$2m$	$\ldots$	$2m$	0

Figure 1. Detour Distance Matrix $(J_{2,m})$

From the above matrix we can easily observe the set W' with $2m-1$ vertices is the detour resolving set with minimum cardinality and $D\beta(J_{2,m}) = 2m-1$.

Theorem 2.2. *For the Fan graph $F_{m,n}$, $m,n \geq 2$, $D\beta(F_{m,n}) = \begin{cases} m+n-1, & m \neq n \\ m+n-2, & m = n \end{cases}$.*

Proof. Let $V(F_{m,n}) = \{u_i/1 \leq i \leq m+n\}$ and $E(F_{m,n}) = \{u_i u_j/i = 1$ to $n-1, j = i+1\} \cup \{u_i u_j/i = 1$ to $n, j = n+1$ to $n+m\}$ be the vertex set and edge set of the Fan graph $F_{m,n}$, respectively. For $m \neq n$, $D(u_i,u_j) = m+n-1$, $i \neq j$. The set W' with any $m+n-1$ vertices is the detour resolving set with minimum cardinality and $D\beta(F_{m,n}) = m+n-1$. For $m = n$, $D(u_i,u_j) = m+n-2$, $i = j = 1,2,\dots,n$, $i \neq j$ otherwise $D(u_i,u_j) = m+n-1$. Then the set W' with any $m+n-2$ vertices is the detour resolving set with minimum cardinality and $D\beta(F_{m,n}) = m+n-2$. □

Theorem 2.3. *For the Friendship graph F_n, $n \geq 2$, $D\beta(F_n) = n$.*

Proof. Let $V(F_n) = \{u_i/1 \leq i \leq 2n+1\}$ and $E(F_n) = \{u_1u_i/2 \leq i \leq 2n+1\} \cup \{u_iu_{i+1}/i = 2,4,6,\dots,2n\}$ be the vertex set and edge set of the Fan graph F_n, $n \geq 2$. Also $D(u_1,u_i) = 2$, $i = 2,\dots,2n+1$ and

$$D(u_i,u_j) = \begin{cases} 2, & \text{if } u_i \text{ and } u_j \text{ are, adjacent} \\ 4, & \text{if } u_i \text{ and } u_j \text{ are non adjacent.} \end{cases}$$

Then the set $w' = \{u_i/$ either $i = 2,4,6,\dots,2n$ or $i = 3,5,7,\dots,2n+1\}$ is the detour resolving set with minimum cardinality and $D\beta(F_n) = n$. □

Theorem 2.4. *For the wheel graph $W_{n,m}$, $n \geq 3$, $1 \leq m \leq n$, $D\beta(W_{n,m}) = \begin{cases} m+n-1, & \text{if } m \neq n \\ m+n-2, & \text{if } m = n. \end{cases}$*

Proof. Let $V(W_{n,m}) = \{u_i/1 \leq i \leq n+m\}$ and $E(W_{n,m}) = \{u_iu_{i+1}/1 \leq i \leq n-1\} \cup \{u_iu_j/n+1 \leq i \leq n+m, 1 \leq j \leq n\}$, be the vertex set and edge set of the Wheel graph $W_{n,m}$, $n \geq 3$, $1 \leq m \leq n$.

If $m \neq n$, then $D(u_i,u_j) = m+n-1$, $1 \leq i \leq n+m$, $1 \leq j \leq n+m$, $i \neq j$ and if $m = n$, then

$$D(u_i,u_j) = \begin{cases} m+n-2, & 1 \leq i \leq n,\ 1 \leq j \leq n,\ i \neq j \\ m+n-1, & n+1 \leq i \leq n+m,\ n+1 \leq j \leq n+m,\ i \neq j. \end{cases}$$

The set W' with any $m+n-1$ vertices is the detour resolving set with minimum cardinality and $D\beta(W_{n,m}) = m+n-1$ for $m \neq n$ and the set W' with any $n-1$ vertices from $u_1,u_2,\dots,u_n$ and $m-1$ vertices from $u_{n+1},u_{n+2},\dots,u_{n+m}$ is the detour resolving set with minimum cardinality and $D\beta(W_{n,m}) = n+m-2$ for $m = n$. □

Theorem 2.5. *For the Circulant graph $C_n(S)$, where $S \subset \left\{1,2,\dots,\left\lfloor \frac{n}{2} \right\rfloor\right\}$, $D\beta(C_n(S)) = n-1$.*

Proof. Let $V(C_n(S)) = \{u_i/1 \leq i \leq n\}$ and $E(C_n(S)) = \{u_iu_j/|u_i - u_j| \equiv s(\text{mod } n), s \in S\}$ be the vertex set and edge set of the Circulant graph $C_n(S)$. Let $u,v \in V$. Then $D(u_i,u_j) = n-1$, $i \neq j$. Therefore, the set W' with any $n-1$ vertices forms the detour resolving set with minimum cardinality and $D\beta(C_n(S)) = n-1$. □

Theorem 2.6. *If $n \geq 2$ is an integer, $p_1,p_2,\dots,p_i$ are prime numbers $(\leq n)$ and α_i is the largest positive integer such that $p_i^{\alpha_i} \leq n$, then the detour metric dimension of the Mangoldt graph M_n is $n-1$.*

Proof. Let $V(M_n) = \{u_i/1 \leq i \leq n\}$ and $E(M_n) = \{u_iu_j/\Lambda(u_i \cdot u_j) = 0\}$ be the vertex set and edge set of the Mangoldt graph M_n. Let $u,v \in V$. Then $D(u,v) = n-1$, $u \neq v$. Therefore the set with any $n-1$ vertices forms the detour resolving set with minimum cardinality and $D\beta(M_n) = n-1$. □

3. Detour Metric Dimension for Some Regular Bipartite Graphs and Corona Product Graph

Theorem 3.1. *For $n \geq 3$, if $G(n,n)$ is an $(n-1)$ regular bipartite graph, then $D\beta(G) = 2n-2$.*

Proof. Let $V(G) = \{u_i/1 \leq i \leq 2n\}$ be the vertex set of $G(n,n)$. Suppose that the set W' contains at most $2n-3$ vertices. Let $u,v,w \in V \setminus W'$. Then at least any two representation from $R(u|W')$, $R(v|W')$ and $R(w|W')$ are equal. Therefore W' contains at least $2n-2$ vertices and $D\beta(G) = 2n-2$. For example, for the graph $G(4,4)$, $W' = \{u_2, u_3, \dots, u_7\}$ is the detour resolving set with minimum cardinality. □

Theorem 3.2. *For $n \geq 3$, if $G(V_1,V_2)$ where $V_1 = \{u_1, u_2, \dots, u_n\}$ and $V_2 = \{v_1, v_2, \dots, v_n\}$ is an $(n-1)$ regular bipartite graph and W' is the set with $n-1$ vertices in V_1 and $n-1$ vertices in V_2, then W' is the detour basis of G.*

Proof. Let $W' = \{u_1, u_2, \dots, u_{n-1}, v_1, v_2, \dots, v_{n-1}\}$. Since $D(u_i,u_j) = n-2$, $1 \leq i,\ j \leq n-1$, $i \neq j$, $D(v_i,v_j) = n-2$, $1 \leq i,\ j \leq n-1$, $i \neq j$ and $D(u_i,v_j) = D(v_i,u_j) = n-1$, $1 \leq i,\ j \leq n-1$, then for every two distinct vertices $u,v \in V$, where $V = V_1 \cup V_2$ should satisfy $R(u|W') \neq R(v|W')$. Therefore, W' is the detour basis of G. □

Theorem 3.3. *For $n \geq 6$, if G is an $n-2$ regular graph, then $D\beta(G) = n-1$.*

Proof. The proof is obvious, Since G is $n-2$ regular graph and $D(u,v) = n-1$, $\forall\ u,v \in G$. □

Theorem 3.4. *For Corona product graph $C_n \odot mK_1$, $n \geq 10$ and $m \geq 1$,*

$$D\beta(C_n \odot mK_1) = \begin{cases} 3, & n \geq 10 \text{ and } m = 1 \\ n(m-1), & n \geq 10 \text{ and } m \geq 2. \end{cases}$$

Proof. Let $V(C_n \odot mK_1) = \{u_i/1 \leq i \leq n(m+1)\}$ and

$$E(C_n \odot mK_1,) = \{u_i u_{i+1}/1 \leq i \leq n-1\} \cup \{u_n u_1\} \cup \{u_i u_j/1 \leq i \leq n, n+(i-1)m+1 \leq j \leq n+im\}$$

be the vertex set and edge set of the Corona product graph $C_n \odot mK_1$, $n \geq 10$ and $m \geq 1$. For $m = 1$, the set W' with any three vertices from $u_1, u_2, \dots, u_n$ with the distance between any two is atleast $\frac{n}{4}$ is the detour resolving set with minimum cardinality and $D\beta(C_n \odot K_1) = 3$. For $m \geq 2$, the set $W' = \{u_i/kn+1 \leq i \leq kn+(m-1), 1 \leq k \leq n\}$ is the detour resolving set with minimum cardinality $D\beta(C_n \odot mK_1) = n(m-1)$, $n \geq 10$ and $m \geq 2$.

Therefore, $$D\beta(C_n \odot mK_1) = \begin{cases} 3, & n \geq 10 \text{ and } m = 1 \\ n(m-1), & n \geq 10 \text{ and } m \geq 2. \end{cases}$$ □

Encryption and Decryption Procedures

The detour path resolvability represents the distinct vertex of graph has distinct code with respect to the detour resolving setW'. This code can be used for divergent approach of secure secrete sharing. In this section we give the procedure and illustration for encryption and decryption.

Procedure.

1. Find the detour path resolving set with distinct code for each vertex of a graph.
2. Assign alphabets $(a,b,c,\dots,z)$, numbers $(0,1,2,3,4,5,6,7,8,9)$, special characters such as $!,@,\#,\$,\%,\&,*,-,+,=,/$ and space bar to the codes corresponding to vertices of the graph $C_n \odot mK_1$, $n \geq 10$ and $m = 1$ in ascending order.
3. To set Cipher text from Encrypted plaintext using
$$f(a,b,c,\dots,z,0,1,\dots,9,!,\dots,/,(0)) \to (N_a,\dots,N_z,N_0,\dots,N_9,N_!,\dots,N_/,N_{(0)})$$
where $(N_a,\dots,N_z,N_0,\dots,N_9,N_!,\dots,N_/,N_{(0)})$ are the codes of the vertices with respect to the detour path resolving set.
4. Send the encoded message with graph or graph invariant to the receiver with path resolving set.
5. Using the resolving set as key receiver, one can find the code of vertices with respect to W'. Assign alphabets, numbers, special characters and space bar to the code of the vertex of the graph $C_n \odot mK_1$, $n \geq 10$ and $m = 1$ in ascending order.
6. The receiver can decrypt the message using function
$$f^{-1}(N_a,\dots,N_z,N_0,\dots,N_9,N_!,\dots,N_/,N_{(0)}) \to (a,b,c,\dots,z,0,1,\dots,9,!,\dots,/,(0))$$

Illustration. We encrypt the text **demonetization**

Step 1. Consider the graph $C_{24} \odot K_1$ and find the distinct code of the vertices using detour path resolvability as shown in Figure 2.

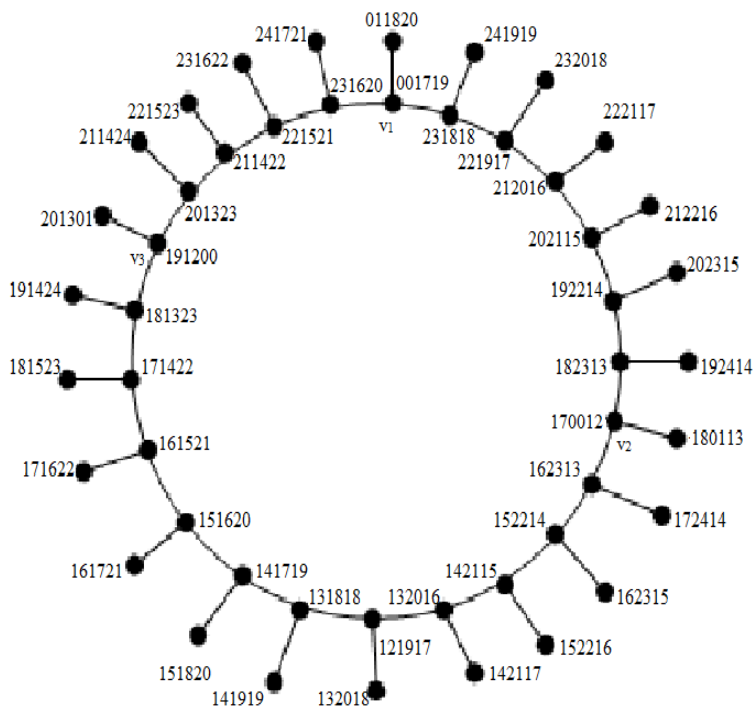

Figure 2. $C_{24} \odot K_1$ with distinct codes

Table 1. Alphabets and symbols with corresponding codes

Code	001719	011820	121917	131818	132016	132018	141719	141919	142115	142117
Letter	a	b	c	d	e	f	g	h	i	j
Code	151620	151820	152214	152216	161521	161721	162313	162315	170012	171422
Letter	k	l	m	n	o	p	q	r	s	t
Code	171622	172414	180113	181323	181523	182313	191200	191424	192214	192414
Letter	u	v	w	x	y	z	0	1	2	3
Code	201301	201323	202115	202315	211422	211424	212016	212216	221521	221523
Letter	4	5	6	7	8	9	!	@	#	$
Code	221917	222117	231620	231622	231818	232018	241721	241919		
Letter	%	&	*	-	+	=	/	(0)		

$*$: $D(v,v)=00$ and $D(u,v)=01$

Step 2. Assign the alphabets, numbers, special characters and space bar(0) to the codes in the ascending order as in Table 1.

Step 3. To get the cipher text by replacing each letter and symbols of plaintext by its corresponding code using Table 1.

Step 4. Send the cipher text and the graph $C_{24} \odot K_1$ with vertex labeling of detour resolving set $W' = \{v_1, v_2, v_3\}$ to receiver.

Step 5. Receiver finds the distinct code using the key W'.

Step 6. Since the detour metric dimension of the graph is three and detour distance between any two vertices is mostly a two digit number, split the block size of cipher text is six. That is

1318181320161522141615211522161320161714221421151823130017191714221421151
61521152216

Step 7. Choose the alphabets and symbols to the codes using Table 1.

The message is **demonetization**.

Competing Interests

The authors declare that they have no competing interests.

Authors' Contributions

All the authors contributed significantly in writing this article. The authors read and approved the final manuscript.

References

[1] M. Baca, E.T. Baskoro, A.N.M. Salman, S.W. Saputro and D. Suprijanto, The metric dimension of regular bipartite graphs, *Bull. Math. Soc. Sci. Math. Roumanie* Tome **54**(102) (1) (2011), 15 – 28.

[2] J. Caceres, C. Hernando, M. Mora, M.L. Puertas, I.M. Pelayo, C. Seara and D.R. Wood, On the metric dimension of some families of graphs, *Electronic Notes in Discrete Math.* **22** (2005), 129 – 133.

[3] G. Chartrand, C. Poisson and P. Zhang, Resolvability and the upper dimension of graphs, *Comput. Math. Appl.* **39** (2000), 19 – 28.

[4] F. Harary and R.A. Melter, On the metric dimension of a graph, *Ars Combin.* **2** (1976), 191 – 195.

[5] V. Kaladevi and P. Backiyalakshmi, Detour distance polynomial of Star Graph and Cartesian product of $P_2 \times C_n$, *Antartica J. Math.* **8**(5) (2011), 399 – 406.

[6] V. Kaladevi and P. Backialakshmi, Maximum distance matrix of super subdivision of star graph, *Journal of Comp. & Math. Sci.* **2**(6) (2011), 828 – 835.

[7] V. Kaladevi and S. Kavithaa, On varieties of reverse wiener like indices of a graph, *Intern. J. Fuzzy Mathematical Archive* **4**(12) (2014), 37 – 46.

[8] V. Kaladevi and S. Kavithaa, Fifteen reverse topological indices of a graph in a single distance matrix, *Jamal Academic Research Journal*, special issue (2014), pp. 1 – 9.

[9] V. Kaladevi and K. Marimuthu, Relation between metric dimension and detour metric dimension for certain graphs, *Jamal Academic Research Journal*, special issue (2014), 441 – 447.

[10] V. Kaladevi and P. Selvaani, Three polynomials in one matrix, *Mathematical Sciences International Research Journal* **1**(1) (2012), 100 – 108.

[11] P.J. Slater, Leaves of trees, *Proc. 6th Southeastern Conf. on Combinatorics, Graph Theory and Computing*, Vol. **14** of Congr. Number, 549 – 559, 1975.

[12] P.J. Slater, Dominating and reference sets in a graph, *J. Math. Phys. Sci.* **22** (1998), 445 – 455.