An Open Access Journal Available Online

Covenant Journal of Informatics & Communication Technology (CJICT)

Vol. 5 No. 1, June, 2017

A Bi-annual Publication of the Departments of Computer Information Science, and Electrical & Information Engineering. Covenant University, Canaan Land, Km 10, Idiroko Road, Ota, Ogun State, Nigeria.

Editor-in-Chief: Prof. Sanjay Misra
sanjay.misra@covenantuniversity.edu.ng

Managing Editor: Edwin O. Agbaike
me@covenantuniversity.edu.ng

Website: http//Journal.covenantuniversity.edu.ng/cjict/

© 2017, Covenant University Journals

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any meams, electronic, electrostatic, magnetic tape, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

It is a condition of publication in this journal that manuscripts have not been published or submitted for publication and will not be submitted or published elsewhere.

Upon the acceptance of articles to be published in this journal,the author(s) are required to transfer copyright of the article to the publisher.

ISSN - Print: 2354 – 3566
- Electronics: 2354 – 3507

Published by Covenant University Journals,
Covenant University, Canaanland, Km 10, Idiroko Road,
P.M.B. 1023, Ota, Ogun State, Nigeria

Printed by Covenant University Press

Articles

Covenant Journal of Informatics & Communication Technology. Vol. 5 No. 1, June, 2017

An Open Access Journal Available Online

Parameterised Key Diffusion Approach of AVK Based Cryptosystem

Shaligram Prajapat

International Institute of Professional Studies
Devi Ahilya University Indore
shaligram.prajapat@gmail.com

Abstract- The enhancement of security of information using symmetric key is the demand of industry and society. For sharing huge files and data symmetric key algorithms is first choice. This paper presents sparse matrix based approach (SAVK) for symmetric key based cryptosystem, exploiting location information for enciphering and deciphering of user's information. The sparse based method has been analyzed with three variants and performance of these approaches has been presented. The benefit of location information for encryption or decryption of information will find its applicability in moving low power gadgets, IOT components and auditing of cryptosystems.

Introduction

Secure information exchange is achieved by cryptographic algorithm. Asymmetric cryptic algorithms are not preferred for big sized files or in formations. Symmetric key based algorithms are suitable for recommended for cloud based information repositories. AES is the first choice as compared to DES, 3DES, BlowFish, RC6 ,Two Fish etc. To improve the performance and increase the degree of security Automatic Variable Key (AVK) based approach has been proposed by (C.T. Bhunia, 2008).Variety of approaches of AVK has been proposed in literature.(Prasun, 2008).Automatic Variable Key (AVK) approach is better alternative over longer sized key. AVK attempts to keep key-size constant and changes entire key in successive sessions. The optimum size of key been approximated up to 7 or 8 characters.(Shaligram and R.S. Thakur, 2015) . One approach of AVK is generation of key using Fibonacci-Q matrix (Shaligram, 2012) where by choosing various terms corresponding to

different values of input parameters new keys of fixed length is generated. Another approach of for moving information sending and receiving equipment using , the location based AVK scheme has been discussed in this paper together with the realization and analysis.(Shaligram Prajapat, 2014) and (Shaligram, 2016). The presented approach exploits the advantage of compact representation of sparse space with key variables using location information based (i, j) information for automatic variable key assuming the situation of moving transmitter and receiver for symmetric key based cryptosystem. The parameters *only* scheme have been used without exchanging entire key and the parameters have been diffused for key-construction using parameters only (shaligram,2016). The subsequent sections, present a scheme based on the sparse matrix approach for efficient and secure communication without using any key exchange.

Definition and Related Work

Sparse Matrix: A matrix of order very high dimension (m x n) having most of its member as zero. The sparse matrix representation schema records information of only non-zero members and discards zero members (Gilbert et. al. 1992). The threshold needed to fall a given square matrix to be "sparse-matrix" depends on the structure of the matrix, number of nonzero members and nature of operations to be performed on it. (W. H., Flannery et.al., 2014). By recording only nonzero member information provides substantial reduction in memory space. Depending on the number and distribution of the non-zero entries, different data structures can be used and yield huge savings in memory when compared to the conventional way of information representation. Consider matrix A of order 6 by 6.

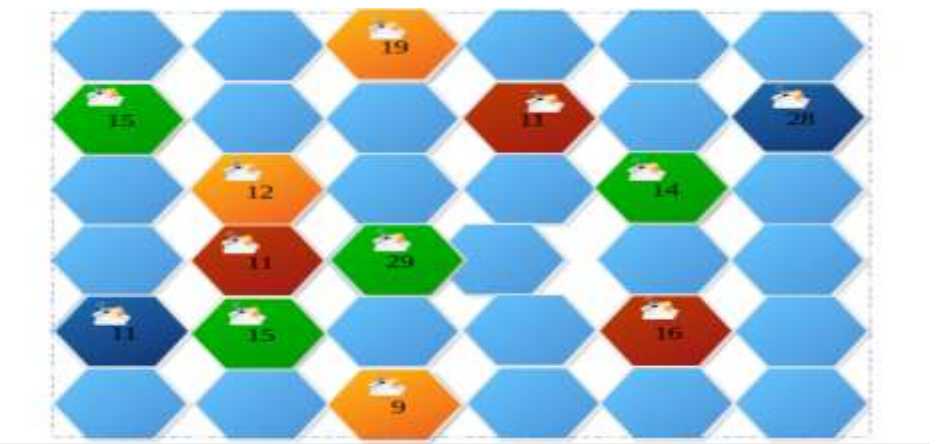

Figure 1: Physical location of data and corresponding data

In Figure 1 the partitioning of a geographical or physical area into small addressable location where moving devices at a location (i, j) exchanging data $d_{ij.}$ The corresponding logical equivalent matrix representation is

shown as matrix A equation (1), where total 12 devices or information sharing nodes are currently located. The locations of these devices are represented as nonzero entry in the sparse matrix and only these information is recorded in compact representation of sparse matrix. The equivalent sparse matrix of figure 1

.

$$A = \begin{bmatrix} 0 & 0 & 19 & 0 & 0 & 0 \\ 15 & 0 & 0 & 11 & 0 & 28 \\ 0 & 12 & 0 & 0 & 14 & 0 \\ 0 & 11 & 29 & 0 & 0 & 0 \\ 11 & 15 & 0 & 0 & 16 & 0 \\ 0 & 0 & 9 & 0 & 0 & 0 \end{bmatrix} \quad (1)$$

The Compact Sparse Matrix (CSM) representation of Sparse Matrix is equation (2).

$$CSM = \begin{array}{l} \text{Header row} \rightarrow \\ \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \\ 10 \\ 11 \\ 12 \\ 13 \end{array} \begin{bmatrix} 6 & 6 & 12 \\ 0 & 2 & 19 \\ 1 & 0 & 15 \\ 1 & 6 & 28 \\ 1 & 3 & 11 \\ 1 & 5 & 18 \\ 2 & 1 & 12 \\ 2 & 4 & 14 \\ 3 & 1 & 11 \\ 3 & 2 & 29 \\ 4 & 0 & 11 \\ 4 & 1 & 15 \\ 4 & 4 & 16 \\ 5 & 2 & 19 \end{bmatrix} \quad (2)$$

By definition a sparse matrix may contain most of the member as zero, but actually what threshold is to be considered during implementation to be taken as a sparse matrix, is given by equation (4).

Necessary condition for being sparse matrix

Let ‘p’ denotes the count of nonzero members of A. For static memory allocation array A of size p would require 3-members (3-tuple) array storage for each nonzero member. To

estimate reduction in storage space using compact way having only record of nonzero members using such representation let us compute total space required for storing A , m x n integer-members in a 2-D array. Obviously,

$$Number of bytes required by A = \text{No.of rows (m)} * No.of columns(n) * Size\_of\_integer \quad (3)$$

In CSM-version of spmat the memory efficiency can be achieved iff:

$$3 * p * Size\_of\_integer\_inBytes \leq m * n * Size\_of\_integer\_inBytes$$

$$p \leq \frac{m*n}{3} \quad (4)$$

In other words, when total count of non-zero members is not exceeding 33% of the total count of members of entire matrix, then the compact storage representation of sparse structure would be beneficial. The matrix A may be represented more economically (in terms of space) using CSM if the conventional 2-D array representation of matrices is not used. Instead it is using representation of only non zero members only. Since 6 X 6 is the order of illustration of Figure 1. Using matrix "A", such that: no_of_rows(m) = 6 :no_of_columns(n) = 6 :no_of_member (Non zero entries p) = 12. This can be expressed also in the [0] position of following spmat array: csm [0][0]. Nonzero members of the array A from index [1...no_of_member] is denoted as:{0, 2, 19; 1, 0, 15; 1, 3, 11; 1, 5, 18; 2, 1, 12; 2, 4, 14; 3, 1, 11; 3, 2, 29; 4, 0, 11; 4, 1, 15; 4, 4, 16; 5, 2, 9 }. (Here notation '{ ' and '}' has been used for array to avoid confusion from reference /citation).CSM [ ][ ] information about a nonzero member has three parts:

1. An integer representing its row_index(i) or CSM[i][0].
2. An integer representing its column_index(j) or CSM[i][1].
3. The nonzero data associated with (i, j)_ location is dij or CSM[i][2].

Such a 3-tuple can be represented by a data structure with 3 fields:

$$csm[1]=[0,2,19],\ csm[2]=[1,0,15],\ csm[3]=[1,3,11],\ csm[4]=[1,5,18],$$
$$csm[5]=[2,1,12],\ csm[6]=[2,4,14],\ csm[7]=[3,1,11],\ csm[8]=[3,2,29],$$
$$csm[9]=[4,0,11],\ csm[10]=[4,1,15],\ csm[11]=[4,4,16],\ csm[12]=[5,2,9]\ \ldots$$

This representation not only saves memory but also stores key parameters that have been diffused in the first and second column of compact sparse matrix CSM[i][0] and CSM[i][1] respectively, where index i is variable subscript holding location of nonzero members in the compact sparse matrix CSM. The transformation of Sparse matrix into Compact Sparse Matrix notation is shown in Figure 2

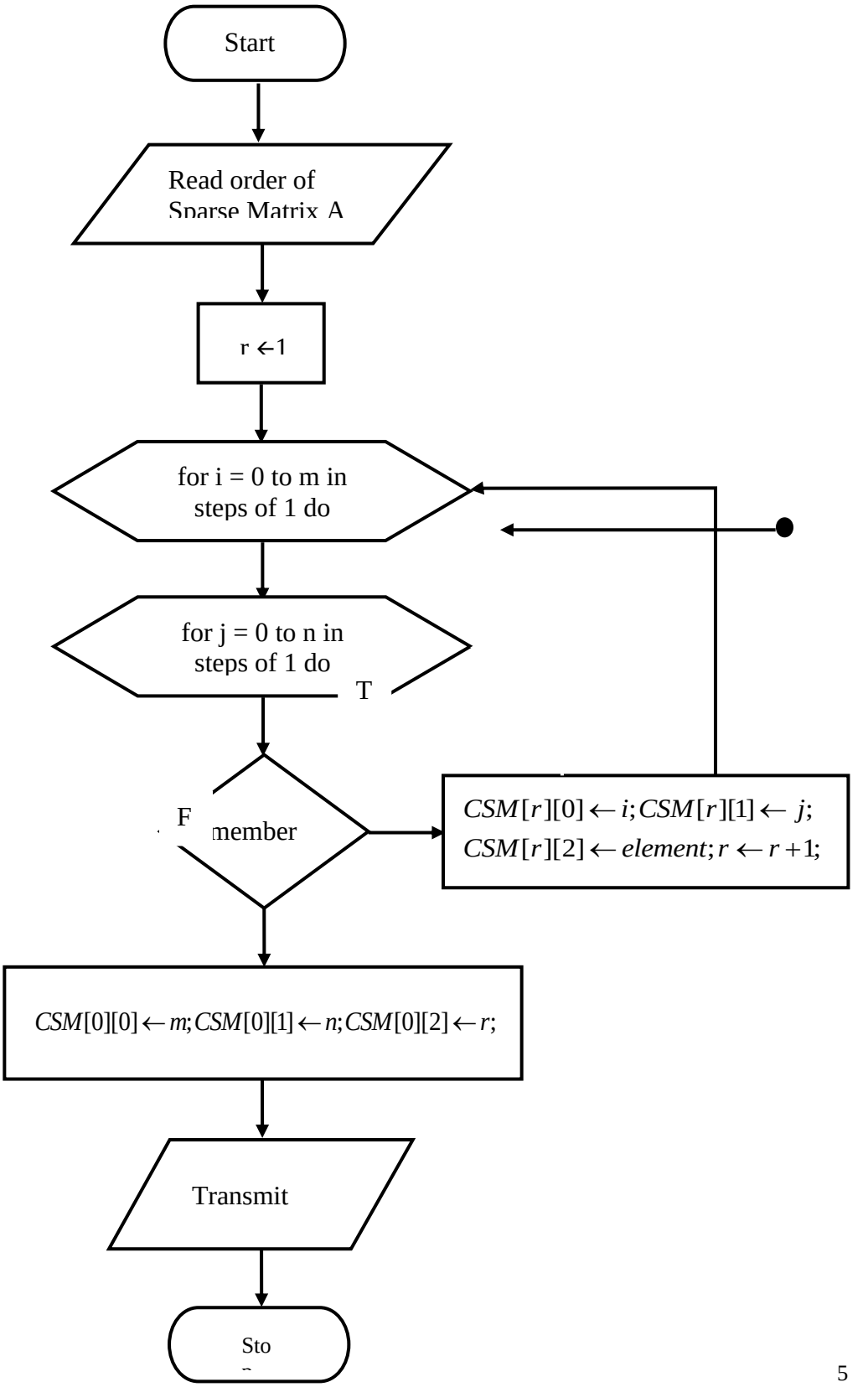
Start
Read order of
Sparse Matrix A
r ←1
for i = 0 to m in
steps of 1 do
for j = 0 to n in
steps of 1 do
T
F
member
CSM[r][0] ← i; CSM[r][1] ← j;
CSM[r][2] ← element; r ← r +1;
CSM[0][0] ← m; CSM[0][1] ← n; CSM[0][2] ← r;
Transmit
Sto

Figure 2: Transformation of Sparse Matrix into Compact Sparse Matrix (CSM)

Proposed Model of Encryption and Decryption (Diffused Parameters for Key SPARSE-AVK Algorithm)

This approach uses Linear Sparse based Symmetric AVK method (LSAVK) in Figure 3, Quadratic Sparse based Symmetric AVK method (QSAVK) in Figure 4 and Cubic Sparse based Symmetric AVK method (CSAVK) in Figure 5, for encryption and decryption using 1-dimensional,2-Dimensional,3-dimensional transformations using location parameters (i, j). Assuming the standard representation scheme the proposed algorithms works with row and column indexes starting from 1.

Proposed Algorithms for Ensuring Security

The transformations from plaintext to cipher text and recovery of plaintext from receiving cipher text will be done by from equations 5, to equation 10.

Linear Sparse AVK based Cryptic process

For a cipher generation of linear transmission using location parameters

$$ciphertext\_CSM'[i][2] = a + b * plaintext \quad (5)$$

For reconstruction of plain text from transformed linear ciphers using location parameters

$$plaintext\_CSM[i][2] \leftarrow \frac{CSM'[i][2] - CSM'[i][0]}{CSM'[i][1]} \quad (5)$$

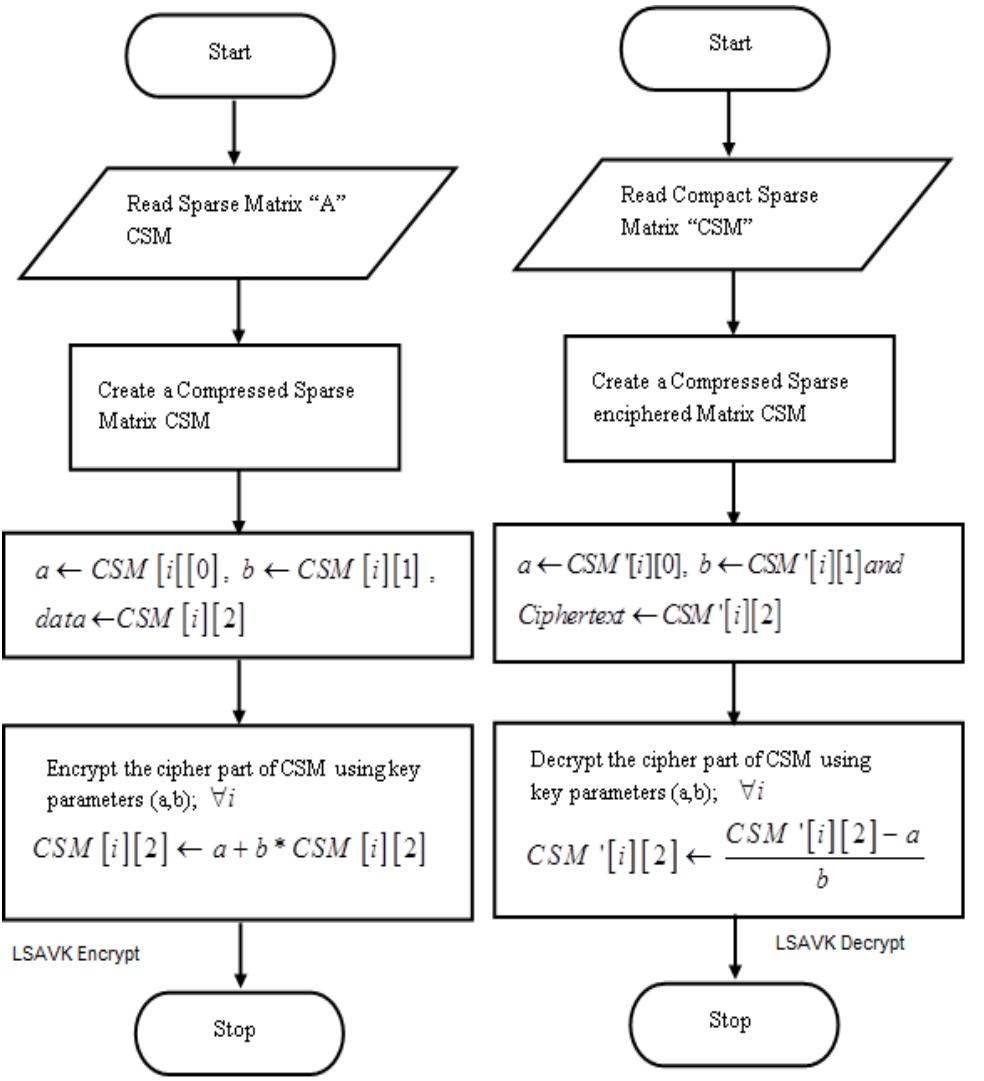

Figure 3: Proposed Cryptic Process for LSAVK

Quadratic Sparse based AVK Process (QSAVK)

For cipher generation of quadratic transformation location parameters

$$ciphertext = a + b * data + (a + b)^2 * data \quad (7)$$

For regeneration of plain text information from quadratic transformed cipher text

$$plain\ \text{text} = \frac{ciphertext - a}{b + (a + b)^2} \quad (8)$$

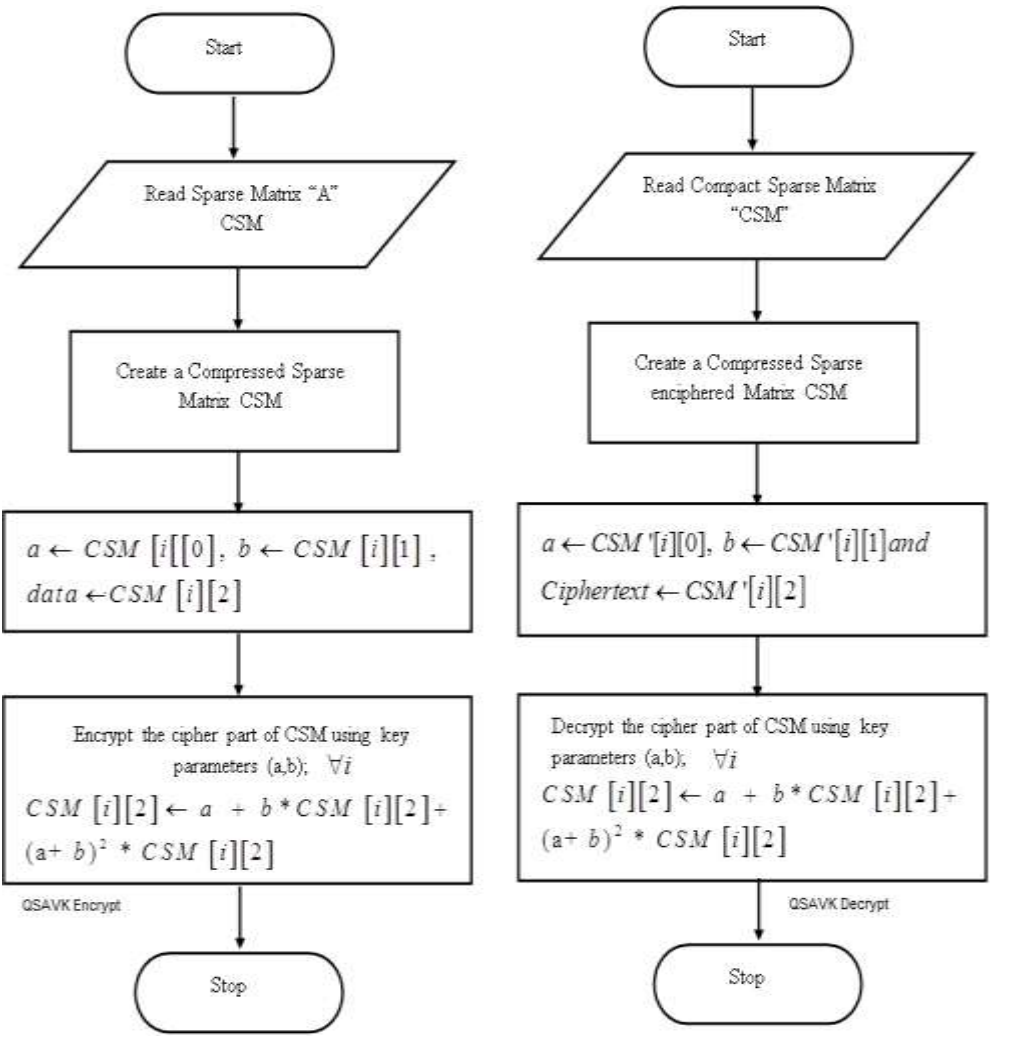

Figure 4: Proposed Process for transformation using QSAVK

Cubic AVK based Cryptic Process (CSAVK)

For cipher generation of cubic transformation location parameters

$$ciphertext = a + b * data + (a+b)^2 * data + (a+b)^3 * data \quad (9)$$

For regeneration of plain text information from cubic transformed cipher text

$$plain\ \text{text} = \frac{ciphertext - a}{b + (a+b)^2 + (a+b)^3} \quad (10)$$

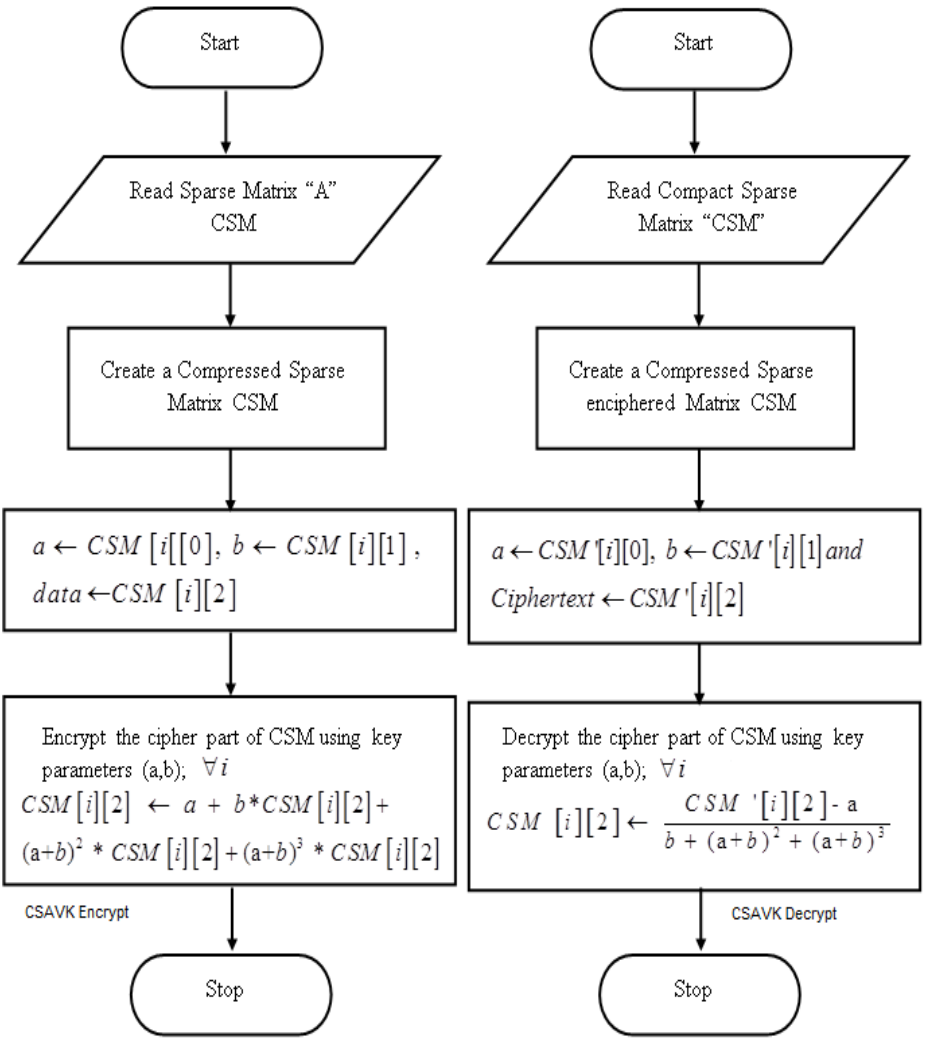

Figure 5: Proposed Process for transformation using CSAVK

Proposed Sparse Based AVK Algorithms (SAVK)

This section presents three cryptic algorithm based on linear(1-D),Quadratic(2-D) and Cubic (3-D) with encryption and decryption functionalities namely, LSAVKEncrypt( ) and LSAVKDecrypt( ) (Algorithm 1 and Algorithm 2) uses linear transformation ,QAVKEncrypt( ) and QSAVKDecrypt( ) (Algorithm 3 and Algorithm 4) uses quadratic transformation and CSAVKEncrypt( ) and CSAVKDecrypt( ) (Algorithm 5 and Algorithm 5) using cubic transformation under proposed Sparse based Symmetric Encryption /Decryption *(LSAVK Figure* 4, *QSAVK Figure* 5, *and CSAVK Figure* 5*)Schemes).*

Encryption Using Linear Transformations(1-D)

Algorithm1 LSAVK-Encrypt (Matrix CSM[ ])

{ // Receive plain text from sender with location information, generate cipher and transmit

for each i from 1 to CSM[0][3] in steps of 1 do

{ a ← CSM[i][0], b ← CSM[i][1], plaintext ← CSM[i][2];

Generate Cipher Text CSM'[i][2] ← a+b*plaintext;

Transmit Cipher Text(CSM'[ ])

}

}

Decryption Using Linear Transformations(1-D)

Sparse based Symmetric Decryption algorithms

Algorithm 2 LSAVK-Decrypt (Matrix CSM'[ ])

{ // Receive compact sparse matrix(cipher text) and recover plaintext information

for each i from 1 to CSM[0][2] in steps of 1 do

{ a ← CSM'[i][0], b ← CSM'[i][1], plaintext ← CSM'[i][2];

Generate Plain Text CSM'[i][3] ← (*CSM* '[*i*][3] – *CSM* '[*i*][0]) / *CSM* '[*i*][1];

return Plain-Text(CSM'[ ])

}

}

Encryption Using Quadratic Transformations(2-D)

Algorithm 3 QSAVK-Encrypt (matrix CSM[ ])

{ // Receive plain text from sender with location information

// and generate cipher and transmit

for each i from 1 to CSM[0][3] in steps of 1 do

{ a ← CSM[i][0], b ← CSM[i][1], plaintext ← CSM[i][2];

Generate Cipher Text CSM'[i][2] ← a+b*plaintext+$(a+b)^2$*plaintext;

Transmit Cipher Text(CSM'[ ])

}

}

Decryption Using Quadratic Transformations (2-D)

Algorithm 4 QSAVK-Decrypt (matrix CSM'[ ])

{

// *This algorithm accepts Compact Sparse Matrix with cipher text*

// and *recovers plain text in plaintext _ CSM'*[*i*]

for each i from 1 *to CSM* '[0][2] *do*

{

Set $a \leftarrow CSM'[i][0],\ b \leftarrow CSM'[i][1],\ plainText \leftarrow CSM'[i][2];$

Generate plainText _ CSM $'[i] \leftarrow \frac{CSM'[i][2] - CSM'[i][0]}{CSM'[i][1] + (CSM'[i][0] + CSM'[i][1])^2};$

return(*PlainText _ CSM* '[ ]);

}

}

Encryption Using Cubic Transformations(2-D)

Algorithm 5 CSAVK-Encrypt (matrix CSM[ ])

{ // Receive plain text from sender with location information

// and generate cipher and transmit

for each i from 1 to CSM[0][3] in steps of 1 do

{ a ← CSM[i][0], b ← CSM[i][1], plaintext ← CSM[i][2];

Generate Cipher Text CSM'[i][2] ← a+b*plaintext+$(a+b)^2$*plaintext+

$(a+b)^3$*plaintext;

Transmit Cipher Text(CSM'[ ])

}

}

Decryption using Cubic Transformations (2-D)

Algorithm 6 CSAVK-Decrypt (matrix CSM'[ ])

{

// *This algorithm accepts Compact Sparse Matrix with cipher text*

// and *recovers plain text in plaintext _ CSM'*$[i]$

for each i from 1 *to CSM'*$[0][2]$ *do*

{

Set a $\leftarrow$ *CSM'*$[i][0]$, *b* $\leftarrow$ *CSM'*$[i][1]$, *plainText* $\leftarrow$ *CSM'*$[i][2]$;

Generate plainText _ CSM'$[i] \leftarrow \frac{CSM'[i][2]-CSM'[i][0]}{CSM'[i][1]+(CSM'[i][0]+CSM'[i][1])^2+(CSM'[i][0]+CSM'[i][1])^3}$;

return(*PlainText _ CSM'*[ ]);

}

}

Analysis of LSAVK, QSAVK, CSAVK with Variation in Input File Size, Size of Parameters

The algorithm Linear AVK Encrypt (), Quadratic AVK Encrypt and Cubic AVK Encrypt accept compact form of sparse matrix entries and use location (index position) as a parameter for Cipher generation i.e. these algorithms utilize location information of nonzero member and converts the information into cipher text in linear, quadratic and cubic way. Similarly Linear AVK Decrypt () receives cipher text of the data item and based on its key (using the index position of the member as parameter) it recover, Quadratic AVK Decrypt ( ), Cubic AVK Decrypt ( ) original information. Since the key is not transmitted in the data transfer. So it becomes highly difficult to interpolate any information regarding plaintext or key. Table-1, Table 2 and Table 3 demonstrates the working of the proposed SAVK scheme. The sparse matrix recovered by Trudy (man in the middle) will be as follows:

{0,2,19; 1,0,15; 1,3,11; 1,5,18; 2,1,12; 2,4,14; 3,1,11; 3,2,29; 4,0,11; 4,1,15; 4,4,16; 5,2,9 }.

The data member corresponding to table-entries at row no. 3, 7 and 9 are same but after enciphering they are represented by different bit strings, this hides patterns of input plain text and making cryptic mining process hard. Since data enciphering is achieved by the location parameter (i, j) of device or data item, therefore the key would be variable and will change automatically for moving device. This variable key is making same data to become different cipher at different locations. Ciphers making position based variability in data items. LSAVK() is memory efficient due to storage of nonzero members only , $O(p+1) = O(p)$ and takes $O(n)$ time for processing, where p is number of nonzero items. Tables 1, Table 2 and Table 3 demonstrates working of cryptic algorithms LSAVK ( ), QSAVK ( ) and CSAVK( ) from sender (column-5 : Data Sent by Alice (Hex code)),Receiver(column-8: Data Received by BOB

(Recovered Text)) and man in middle (Column-6: Message bits on Noisy Channel).

Table 1: Illustration of LSAVK based Information Transmission

Index	i	j	M(i,j)	Data Sent by Alice (Hex code)	Message bits on Noisy Channel	Cipher on channel	Data Received by BOB (Recovered Text)
0	6	6	12	0C	00001110	4E	0C
1	1	3	19	13	00111010	3A	13
2	2	1	15	0F	00010001	11	0F
3	2	4	11	0B	00101110	2E	0B
4	2	6	18	12	01101110	6E	12
5	3	2	12	0C	00011011	1B	0C
6	3	5	14	0E	01001010	49	0E
7	4	2	11	0B	00011010	1A	0B
8	4	3	29	1D	01011011	5B	1D
9	5	1	11	0B	00010000	10	0B
10	5	2	15	0F	00100011	23	0F
11	5	5	16	10	01010101	55	10
12	6	3	09	09	00100001	21	09

Table 2: Illustration of QSAVK based Information Transmission

Index	I	j	M(i,j)	Data Sent by Alice (Hex Code)	Message bits on Noisy Channel	Cipher on Channel	Data Received by BOB (Recovered Hex Code)
0	6	6	12	0C	011100001110	70E	0C
1	1	3	19	13	000101101010	16A	13
2	2	1	15	0F	000010011000	098	0F
3	2	4	11	0B	000110111010	1BA	0B
4	2	6	18	12	010011101110	4EE	12
5	3	2	12	0C	000101000111	147	0C
6	3	5	14	0E	001111001001	3C9	0E
7	4	2	11	0B	000110100110	1A6	0B
8	4	3	29	1D	010111101000	5E8	1D
9	5	1	11	0B	000110011100	19C	0B

10	5	2	15	0F	001100000010	302	0F
11	5	5	16	10	011010010101	695	10
12	6	3	9	09	001011111010	2FA	09

Table 3: Illustration of CSAVK based Information Transmission

Index	I	j	M(i,j)	Data Sent by Alice (Hex Code)	Message bits on Noisy Channel	Cipher on channel	Data Received by BOB (Recovered Hex Code)
0	6	6	12	0C	0101100000001110	580E	0C
1	1	3	19	13	0000011000101010	062A	13
2	2	1	15	0F	0000001100111101	022D	0F
3	2	4	11	0B	0000101100000010	0B02	0B
4	2	6	18	12	0010100011101110	28EE	12
5	3	2	12	0C	0000011100100011	0723	0C
6	3	5	14	0E	0001111111001001	1FC9	0E
7	4	2	11	0B	0000101011101110	0AEE	0B
8	4	3	29	1D	0010110011010011	2CC3	1D
9	5	1	11	0B	0000101011100100	0AE4	0B
10	5	2	15	0F	0001011100011011	171B	0F
11	5	5	16	10	0100010100010101	4515	10
12	6	3	9	09	0001110010011011	1C9B	09

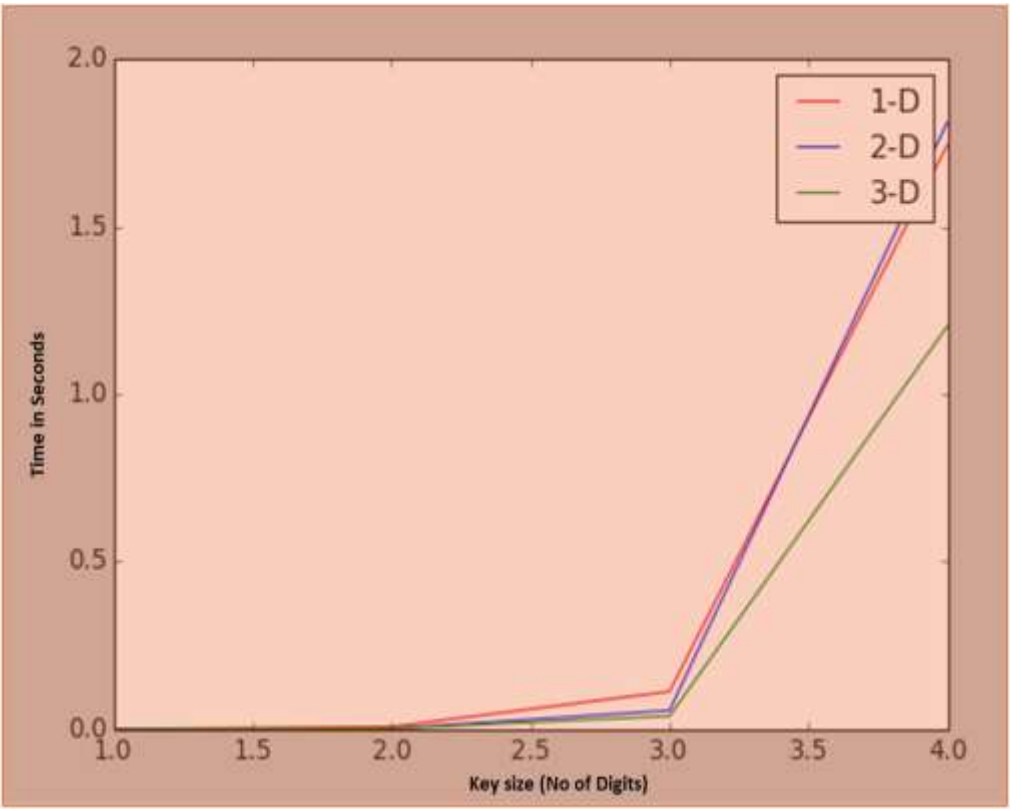

Figure 5: Key Size(X-axis) and corresponding time taken in Seconds(Y-axis) by LSAVK(),QSAVK(),CSAVK()

The performance of LSAVK, QSAVK and CSAVK are shown in figure 5, that shows with increasing the number of digits of parameters from 3 digits onwards the time taken by these algorithms varies fast. In Figure 7 the relative performance of the algorithm is presented, form both the figures it is clear that the performance of CSAVK is better.

Discussions and Future Directions

The encryption algorithms LSAVKEncrypt(), QSAVKEncrypt() and CSAVKEncrypt() use curves of linear, Quadratic and Cubic relationships that are parameterized by a and b. It is worth to check whether these relationships are manifested into produced ciphertext. If yes then it is better to apply rot-13 type of transformation before encryption process. The reverse of it can be applied at recipient end i.e. by LSAVKDecrypt(),QSAVKDecrypt()and CSAVKDecrypt().

Parameter Size (In Number of Digits) v/s. Max. Execution Time

The effect of increasing key size increasing non-linearly when numbers of digits are increased from 3.the table

Table 4: Key size (In Number of Digits) v/s. Execution Time

Key size (number of digits)	Sparse Matrix		
	1 degree decryption Execution Time (sec)	2 degree decryption Execution Time (sec)	3 degree decryption Execution Time (sec)
1	0.0003	0.0002	6.6996
2	0.0019	0.0019	0.0003
3	0.0337	0.0418	0.0346
4	0.7451	1.8633	0.7454

The Performance of Proposed Algorithms with Variable File Size.
In Table 5 demonstration of effect on the decryption time (in seconds) taken for various input size in Bytes. Whereas the Table 5 shows the decryption time (in seconds) taken for various input size in Bytes.

Table 5: Comparative Execution Times (In Sec) of Secret Key Algorithm

Input Size (Bytes)	LSAVK (Sec)	QSAVK (Sec)	CSAVK (Sec)
20527	0.00271	0.00306	0.00394
36002	0.00493	0.00479	0.00556
45911	0.0126	0.00602	0.00677
59862	0.00746	0.00889	0.00834
69646	0.00853	0.00913	0.00963
137325	0.02251	0.01904	0.01921
158959	0.02081	0.02173	0.02217
166364	0.02965	0.02603	0.02621
191383	0.03049	0.03154	0.03126
232398	0.03234	0.03326	0.03330

The result of table 5 is shown in figure 7 and it clears that time required by LSAVK (), QSAVK(), CSAVK( ) increases with increase in file size. The performance of LSAVK is sensitive towards file size whereas QSAVK() and CSAVK() are in close competition. CSAVK() performance is stable over LSAVK() and QSAVK().

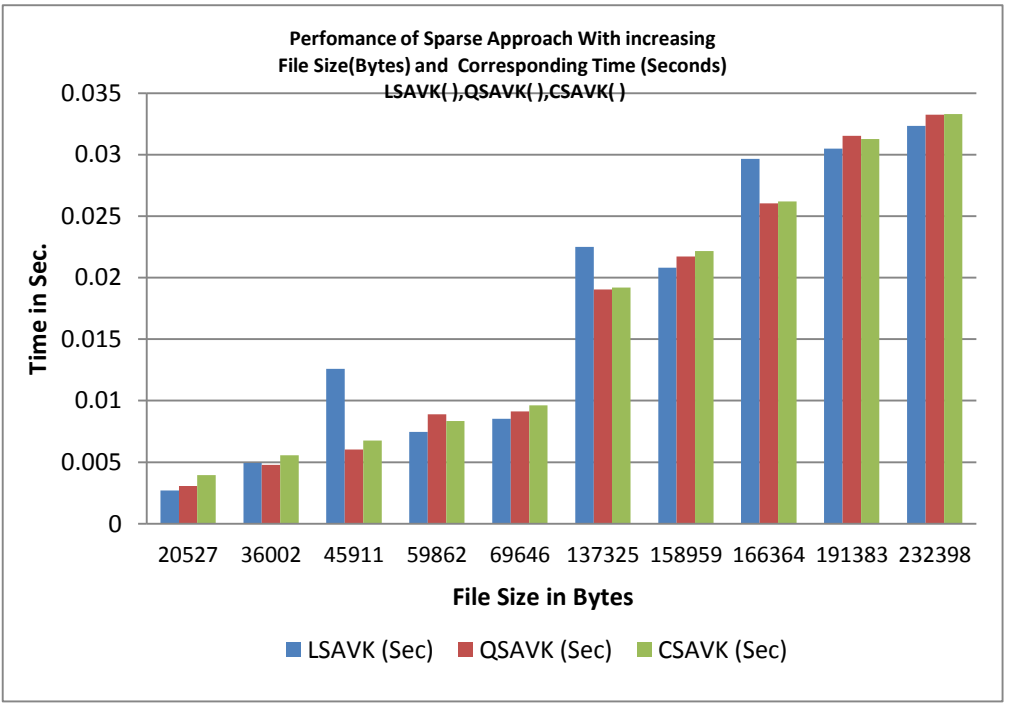

Figure 7: Relative comparison of LSAVK( ),QSAVK( ) and CSAVK( )

Conclusion

This paper presents six cryptic algorithms that apply three different degrees and performance comparison. The relative result comparison of the three approaches show better performance of CSAVK. The beauty of this approach that it does not require key exchange and diffused parameters set for key construction. The proposed technique open new perspectives for secure communication using AVK approach for low power devices together with saving the key computation time.

References

Shaligram Prajapat , Ramjeevan Singh Thakur , "Key Diffusion Approach for AVK based Cryptosystem", In proceedings of Second International Conference on Information and Communication Technology for Competitive Strategies, March 2016. Article No. 78,,ISBN: 978-1-4503-3962-9 doi:10.1145/2905055.2905288.

Shaligram Prajapat, Shashank Swami, Bhagirath Singroli, R. S. Thakur, Ashok Sharma, D. Rajput," Sparse Approach for Realizing AVK for Symmetric Key Encryption", International Journal of Recent Development in Engineering and

Technology
,Vol.2(4), pp. 15-18.June 2014.

Chakrabarti P., Bhuyan B., Chowdhuri A., and Bhunia C., A novel approach towards realizing optimum data transfer and Automatic Variable Key (AVK) in cryptography, IJCSNS International Journal of Computer Science and Network Security, Vol. 8, No. 5, pp. 241, 2008.

Chakrabarti P, "Application of. Automatic Variable Key (AVK) in RSA". Int'l J HIT Transactions on ECCN, Vol.2,. No. 5, Jan-Mar 2007, pp. 304-311.

Chakrabarti et al., Various New and Modified approaches for selective encryption (DES, RSA and AES) with AVK and their comparative study, published in International Journal HIT Transactions on ECCN, Vol 1, No.4, p. 236-244. 51

Bhunia, C. T., Application of AVK and selective encryption in improving performance of quantum cryptography and networks, United Nations Educational Scientific and Cultural Organization and International Atomic Energy Agency, retrieved, Vol.10, No. 12, pp. 200-210, 2006.

Bhunia C. T., New Approaches for Selective AES towards Trackling Error Propagation Effect of AES, Asian Journal of Information Technology, Pakistan, Vol. 5, No. 9, pp. 1017-1022, 2006.

Bhunia C. T., Chakrabarti P., Chowdhuri A. and Chandan T., Implementation of Automatic Variable Key with Choas Theory and Studied Thereof, J IUP Computer Science, Vol -5, No 4, pp. 22-32, 2011.

Bhunia C.T., Mondal G. and Samaddar S., Theories and Application of Time Variant Key in RSA and that with selective encryption in AES, Proc. EAIT, Elsevier Publications, Calcutta CSI-06, pp. 219-221, 2006.

Dutta M.P., Banerjee S. and Bhunia C., Two New Schemes to Generate Automatic Variable Key (AVK) to achieve the Perfect Security in Insecure Communication Channel, Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET 2015), pp.1-4, 2015.

Prajapat, Shaligram, D. Rajput, Ramjeevan Singh Thakur, "Time variant approach towards symmetric key", In proceedings of IEEE Science and Information Conference (SAI), London 2013. , pp.398-405, 2013.

Prajapat, Shaligram, Ramjeevan Singh Thakur. "Optimal Key Size of the AVK for Symmetric Key Encryption." In Covenant Journal of Information & Communication Technology,Vol.3(2), pp. 71-81. 2015.

Prajapat, Shaligram, Ramjeevan Singh Thakur. "Various Approaches towards Crypt-analysis." International Journal of Computer Applications, Vol. 127(14), pp. 15-24, 2015. (doi: 10.5120/ijca2015906518)

Prajapat, Shaligram, Ramjeevan Singh Thakur. "Cryptic Mining for Automatic Variable Key Based

Cryptosystem", Elsevier Procedia Computer Science, Vol. 78 (78C), pp. 199-209, 2016. (doi: doi:10.1016/j.procs.2016.02.034) .

Prajapat, Shaligram, Ramjeevan Singh Thakur."Cryptic Mining: Apriori Analysis of Parameterized Automatic Variable Key based Symmetric Cryptosystem."International Journal of Computer Science and Information Security, Vol. 14 (2), pp. 233- 246, 2016.

Prajapat, Shaligram, Ramjeevan Singh Thakur. "Realization of information exchange with Fibo-Q based Symmetric Cryptosystem." International Journal of Computer Science and Information Security ,Vol 14(2), pp. 216-223, 2016.

Prajapat, Shaligram, Thakur, A., Maheshwari, K., & Thakur, R. S., "Cryptic Mining in Light of Artificial Intelligence", IJACSA , Volume 6(8), pp. 62-69, 201510.14569/IJACSA.2015.060808) .

Prajapat shaligram (2016), Towards parameterized shared key for AVK approach, Chapter 4 ,Pattern and Data Analysis in Health care settings, IGI Global Publications.

W. H., Flannery, B. P., Teukolsky, S. A., Vetterling, W. T. "Sparse Linear Systems. in Numerical Recipes in FORTRAN: The Art of Scientific Computing", 2nd ed. Cambridge, England: Cambridge University Press, pp. 63-82, 1992.

Tim Davis, http://mathworld.Wolfram .com/ topics/ DavisTim.html, April 2014.

Gilbert, J. R, Moler, C. Schreiber, R., "Sparse Matrices in MATLAB: Design and Implementation", SIAM J. Matrix Anal. Appl. 13, 333-356, 1992.

Covenant Journal of Informatics & Communication Technology. Vol. 5 No. 1, June, 2017

An Open Access Journal Available Online

Integration of Non-Motorized Transportation to Rosslyn and Ga-Rankuwa Corridor of Tshwane, South Africa

Mongamo Jantjies[1], Julius Ndambuki[2], Williams Kupolati[3], Adeyemi Adeboje[4] & Chewe Kambole[5],

[1]Department of Civil Engineering,
Tshwane University of Technology, Pretoria, South Africa
mongamojantjies@gmail.com
[2]Department of Civil Engineering,
Tshwane University of Technology, Pretoria, South Africa
NdambukiJM@tut.ac.za
[3]Department of Civil Engineering,
Tshwane University of Technology, Pretoria, South Africa
KupolatiWK@tut.ac.za
[4]Department of Civil Engineering,
Tshwane University of Technology, Pretoria, South Africa
AdebojeAO@tut.ac.za
[5]Department of Civil Engineering,
Tshwane University of Technology, Pretoria, South Africa
KamboleC@tut.ac.za

Abstract: The requirements of sustainable transportation system are safety, affordability, accessibility and convenience. A sustainable transportation system connects various transport modes to enhance efficient movement. It is environmentally friendly and economical. The non-motorized transportation (NMT) may offer safe, efficient, economical and sustainable movements required if integrated with the transportation system. Walking begins and ends trips taken by public and private transportation means. The origin and destination of a journey cannot be completed except NMT is employed. However, NMT as a mode of transportation is yet to be adequately utilized to achieve sustainable transportation in the city of Tshwane. The main aim of this

research is to determine the optimal transportation means by integrating NMT into the journey between Ga-Rankuwa and Rosslyn. The travel pattern obtained from trip studies of BMW staff between Rosslyn and Ga-Rankuwa was studied and juxtaposed with the integrated transport plan (ITP) and municipal housing survey (MHS) of Tshwane. A linear programming method called simplex technique was utilized for the determination of trip duration and trip cost from the origin-destination study results. The movement records of the BMW staff was optimized. A sensitivity analysis was conducted on the model and the results were evaluated. The result showed that taxi was the most patronized mode of transportation by the BMW staff between Rosslyn and Ga-Rankuwa corridors. The result also showed that the average trip cost of BMW workers from home to office is R18.47. Integration of cycling as a mode of transportation for short distance trips created 3 more trip patterns. When cycling was integrated to the rail transportation, 36% of the transportation cost was reduced. This work also showed that the subsisting trip method may still be used by less than 45% of the BMW staff while more than 55% of the staff may utilize the integration of cycling and train from home to office and vice versa. This research recommends that similar investigation should be done to other routes of economic importance in the City of Tshwane in order to encourage the integration of cycling into transportation from one place to another.

Keywords: Origin-destination study, simplex technique, sustainable transportation, trip duration, trip cost.

1. Introduction

Development of a sustainable transportation system requires integration of various modes of transportation in order to achieve accessible, effective, safe and convenient movements of road users. Victoria Transport Policy Institute (2012) quoted (Beatley, 1995) that there is no specific definition of sustainable transportation as trip purposes and modes of travel are usually not the same. It is very difficult to achieve effective transportation in a developing country because the various needs of the people should be considered in the planning, design and construction of transportation facilities. The European Conference of Ministers of Transport (ECMT) in 2004 defined sustainable transport as a transportation system that is affordable, accessible, environmental friendly and safe (Victoria Transport Policy Institute, 2012).

Examples of non-motorized transport (NMT) are bicycling, walking, wheel chair travel, and skating. Non-motorized transport serves both recreational and transportation purposes. It facilitates the movements of persons and goods. It is a matter of choice for a person to cycle or walk instead of driving, depending on what the interest or choice of the person is. The man may enjoy cycling or walking but detest driving in order to do exercise, not minding the stress or longer time required (Victoria Transport Policy Institute, 2012). Non-motorized transport enhances movement of people and goods through other means apart from using vehicles on the road (Guitink, Holste, & Lebo, 1994).

There is a high number of NMT users across several places but they are not considered in the planning, design and construction of new transportation facilities or improvement of existing ones. There is usually no provision or consideration for NMT in the development of facilities like kerbs, shoulders and overpasses; or rehabilitation of existing transportation corridors. High accident rate, segregation of non-motorized traffic and delayed travel time result from non-integration of NMT in new facilities or rehabilitation of existing ones (Guitink, Holste, & Lebo, 1994). Though non-motorized transportation like walking and cycling are sustainable, their application may be limited to only short journeys (Ison & Ryley, 2007).

Many trips by public and private transport start and end with walking. Non-motorized transport is essential for the completion of trips from the commencement to the end (Unep Transport Unit, 2004). It is yet to be adequately utilized to achieve efficient and sustainable transportation system in the public transport sector. Taxi motorists utilize this opportunity to maximize their profits, as they pick passengers up and drop them off very close to their residences and destinations. The railway transportation is used by public passengers but its operation is still below its capacity when compared to how passengers patronize the taxi. The taxi is greatly patronized at the expense of the rail because of passenger's mentality that the rail is not as accessible to the public as Taxi in the Tshwane region (City of Tshwane, 2007).

Tshwane residents are confronted with challenges of expensive transportation cost and inadequate feeder modes to connect the different types of transportation means. The experience of residents of North West part, in Mabopane, Ga-Rankuwa and Soshanguvhe areas is not different (City of Tshwane, 2013).

A comprehensive rail network for the city is available but not fully utilized. If the rail system is fully explored it may make transportation more accessible, easier, efficient and more economical. Many passengers go to work using the taxis, buses and trains. The target was that workers should spend below ten per cent of their salary on return trip to work. The current scenario shows that forty-one per cent of workers spend beyond the recommended ten per cent on transportation (City of Tshwane, 2007). A cheaper or perhaps more flexible transportation mode is needed to ensure that people do not spend up to ten per cent of their salary on transport. It is important to evaluate the possibility of integrating walking and cycling with the existing transportation scenarios. Many passengers (52%) showed displeasure over using train, as there is usually a very long distance to cover between the train station and their destinations, homes or work places (City of Tshwane, 2007).

The current challenges of the rail transportation are unavailability of accessible, comfortable, economical, effective and safe feeder system which would be closer to residences in order to enhance security; and save time and money. If the situation is improved, more passengers will patronize the rail

system and there will be increased shares obtained from rail transportation system in addition to the achievement of a better and sustainable transportation system (City of Tshwane, 2007). According to Tirachini & Hensher, (2012) when the rail transportation fare is low, car owners are discouraged from using their cars while cyclists and walkers are directed towards the railway system.

Adequate knowledge of non-motorized transportation is required in order to enhance reduction of time and cost of travel. Full understanding of NMT will enhance implementation of optimized transportation resulting from integration of NMT (walking and cycling) with the taxi, bus and train.

The aim of this research was to investigate an optimized integration of transportation modes for trips between Rosslyn and Ga-Rankuwa by BMW workers in order to reduce time and cost of travel. The effects of integrating walking and cycling into the public transportation was evaluated.

2. Methodology

The trip patterns of BMW employees transiting from Rosslyn to Ga-Rankuwa in Tshwane was studied. The results obtained from the origin-destination study were analyzed to obtain the following:

- Origin-Destination
- Trip duration
- Cost of travel and
- Travel distance.

The MHS and ITP records of Tshwane obtained were used to study the travel behaviours of BMW workers. Records obtained from the BMW's department of human resources in addition to results of trips undertaken by the workers were compared with data obtained from City of Tshwane, (2007). Trips undertaken with bicycles, trains and taxis were recorded. The data obtained were analyzed.

The source of secondary information used was adjudged reliable. Primary data obtained from study trip and interview were highly rated. The data obtained varied as the technique used for evaluation assisted in decision making.

Alternative Transport Scenarios

Walking and cycling are the most recognized forms of non-motorized transportation by the government of the Republic of South Africa. Non-motorized transportation is likely to become the practically sustainable and feasible transportation mode in South Africa (City of Johannesburg, 2009).

Non-motorized transportation was projected as the potential mode of transportation. An alternative means of transportation will be developed if NMT is integrated to existing public transportation modes which include buses, bus rapid transit, Gautrain, taxis and SARCC Metrorail (City of Johannesburg, 2009).

Table 1 shows related literature used to develop the alternative modes of transportation. The trip patterns used are as follows:

- TRIP PATTERN 1: Walk to taxi stop; board taxi to taxi rank; board taxi to taxi stop close to BMW; walk to BMW gate 1 (Status quo).
- TRIP PATTERN 2: Cycle to taxi rank; transfer from bicycle to taxi; board taxi to taxi stop close to BMW; walk 200 m to BMW gate 1.

- TRIP PATTERN 3: Cycle to nearest rail station; transfer from bicycle to train; board train and alight at Rosslyn rail station; walk to BMW gate 2.
- TRIP PATTERN 4: Cycle to nearest rail station; transfer to train along with bicycle; board train and alight at Rosslyn rail station; cycle to BMW gate 2.

Relevant literature for alternative transportation modes

Materials	Submissions
Tshwane ITP, 2007	Recommended affordable and reliable feeder transportation modes.
National DoT NMT Policy, 2008	Recommended guidelines for planning and implementation of NMT infrastructures.
National DoT, 2003	Proposed design elements of NMT facilities.

The subsisting trip pattern (status quo) is trip pattern 1. It contains only a trip and was undertaken in a period of over an hour. The trip has a travel distance of over 70 kilometers. Trip pattern 2 comprises trips from four different areas with duration of over an hour. The areas are located at distances more than 10 kilometers away from the taxi rank hence it has longer cycling time. Therefore, trip pattern 2 is not a feasible mode. Trip pattern 3 consists six areas with trip duration of over an hour due to longer cycling or walking. The implication is that cycling and walking are not feasible for those six areas under trip pattern 3. Trip pattern 4 consist two areas having trip duration of over an hour which implies that cycling is not feasible for the two areas under consideration in trip pattern four.

3. Optimization of Transportation

Optimizing the cost of transportation for BMW employees was identified as a means of solving the transportation problem which has been begging for solution. This work was targeted at minimizing or reducing their transportation cost with the use of simplex technique which is a linear programming method. A model of Microsoft excel which uses a solver was developed to solve the transportation problem. A tool present in excel spreadsheet for the solution of optimization problems, non-linear equations or a system of linear and nonlinear equations is called 'Excel solver' (Arora, 2012). A number of trip patterns and their sensitivity analyses results were used to test the model.

Mathematical Formulation

Hypothesize that BMW workers are coming from an origin *m* zones and they have to cover trip pattern *n* before they can get to their destination. The workers have to be transported from their residences to work place. The workers can be grouped from the zone where they are coming from as *s* number of workers. All the workers must cover certain trip pattern *n* to get to where they

are going (destinations). There is a linear relationship for the cost of transportation of the individual trip patterns. The transportation problem has the following characteristics:

- Total number of workers using trip pattern j for transport is d_j, where $j = 1,2,3\ldots n$
- Total number of workers from unit i is S_i, where $i = 1,2,3\ldots m$
- The travelling time for one employee from origin unit i using trip pattern j *is* Tij, where $i = 1,2,3\ldots m$ *and* $j = 1,2,3\ldots n$. The total travelling time is linear with respect to the distance to be travelled.
- Total transportation cost for one employee from origin unit i using trip pattern j is c_{ij}, where $i = 1,2,3\ldots m$ *and* $j = 1,2,3\ldots n$. The total transportation cost is linear with respect to the number of employees.
- The maximum cycling distance K for scenario j is 5km, where $j = 1,2,3\ldots n$.
- The maximum trip duration *is* Tij for scenario j is 60 minutes, where $i = 1,2,3\ldots m$ *and* where $j = 1,2,3\ldots n$.

$Tij \leq 60min$ is a constraint and benchmark set by [7].
$\mathrm{K} = 5\mathrm{km}$, is a constraint recommended by [14] stating 5 km as the maximum acceptable cycling distance.

Let Z be the total cost and x_{ij}, the number of workers to be moved from source i using trip pattern j, the formulation for this problem gives a linear programing as follows:

minimze Z

$$= \sum_{i=1}^{i=m} \sum_{j=1}^{j=n} c_{ij}\, x_{ij} \qquad [1]$$

Dependent on:

$$\sum_{j=1}^{j=n} X_{ij} = S_i, \quad (i = 1 \text{ to } m) \qquad [2]$$

$$\sum_{i=1}^{i=m} X_{ij} = d_j, \quad (j = 1 \text{ to } n) \qquad [3]$$

$$\mathrm{K}_j \leq 5km, \quad (j = 1 \text{ to } n) \qquad [4]$$

$$Tij \leq 60min, \ (i = 1 \text{ to } m \text{ and } (j = 1 \text{ to } n) \qquad [5]$$

and:

$$X_{ij} \geq 0, \quad (i = 1 \text{ to } m \,; j = 1 \text{ to } n)$$

The Objective Function

The cost allotted to individual functions of the variables is referred to as objective function. It results from the problem of reducing or minimizing the cost of transportation from an origin point i using a trip pattern j. In any consideration for i and j, the travel cost of each worker is c_{ij} and the total number of employees to be transported

is X_{ij}. Following the above analysis, there is a linear cost function for the overall cost of trips which is $c_{ij}\, x_{ij}$

The summation of the entire i and j results in the overall cost of transportation for the entire combinations of origins and trip patterns. The objective function is represented as shown in equation [1].

The Constraints or Constrictions can be expressed as conditions that enhances the achievement of demand and supply. Any given transportation problem (TP) possesses a singular constraint at each node. The constrictions or constraints can hence be expressed as follow:

Number of workers from all origins that have to be moved:

The Constrictions

$$\sum_{j=1}^{j=n} X_{ij} = S_i, \quad (i = 1 \text{ to } m) \qquad [2]$$

Number of workers that should get to the end point:

$$\sum_{i=1}^{i=m} X_{ij} = d_j, \quad (j = 1 \text{ to } n) \qquad [3]$$

Limit for cycling distance K is 5km on any pattern:

$$\mathrm{K}_j \leq 5km, (j = 1 \text{ to } n) \qquad [4]$$

Total journey time *Tij* from unit i using trip pattern j should not exceed an hour:

$$Tij \leq 60min, \ (i = 1 \text{ to } m \text{ and } j = 1 \text{ to } n) \qquad [5]$$

Non negativity:

$$\mathrm{X}_{ij} \geq 0, \quad \forall\, i \text{ and } j \qquad [6]$$

An important and sufficient condition for the workable solution to the problem of transportation:

$$\sum_{i=1}^{i=m} S_i = \sum_{j=1}^{j=n} \mathrm{d}_j \qquad [7]$$

This implies that to effectively move all workers successfully from their individual points of origin to their destination point equation [7] apply.

Formulating the Transportation Problem using Excel

Two individual tables were created to solve the problem of transportation. The first one was created to house the parameters while the second one was to display the solution. The total number of employees from each point of origin was allocated to each trip patterns (Table II).

Five constraints (constrictions) were built-in on the excel spreadsheet. The constraints are demand constraint; supply constraint; maximum cycling distance constraint; maximum travelling duration constraint and non-negativity constraint.

For the supply constraint, the total number of employees from the individual areas equaled the total number of employees moved in all trip

patterns. This means that the total number of employees between column C and column F equaled the total number of employees in column B which is the solution table (Table II).

For the demand constriction, the total number of employees to be transported equaled the total number of workers who were from different points of origins or different locations. Row G shows at its end the formula (G49 = SUM G30:G48) which was the calculated total number of employees (inserted) added up to the total number of employees transported (Table II).

Cell H49 shows the calculated total cost of the entire trips. The inserted formula as generated gives the overall cost of corresponding cells in the body of the parameter and the table for solution. Hence, the formula programmed in cell H49 adds up the product of the cells in the costing worksheet as presented in the table for parameters and the applicable cells in the table for solution (Table II).

A simple calculation was made to check if any trip pattern would be achievable using the constraint of cycling distance. This was possible through the addition of the columns for all trip patterns and including cycling in one or more of the legs, showing the cycling distances for each trip patterns and origin (columns E to G of Table III).

Table II: Data for trip patter between Ga-Rankuwa and Rosslyn

	A	B	C	D	E	F	G	H
1		**Parameters Table**						
2			COST					
3								
4	**Source / Origin**	**No. of People / Supply**	**Trip Pattern 1**	**Trip Pattern 1**	**Trip Pattern 1**	**Trip Pattern 1**		
5	Barseba	1	R 49,00	R 16,00	R 10,50	R 12,50		
6	Garankuwa View	3	R 42,00	R 48,00	R 25,50	R 31,50		
7	Garankuwa Zone 1	3	R 42,00	R 48,00	R 25,50	R 31,50		
8	Garankuwa Zone 16	6	R 84,00	R 96,00	R 51,00	R 63,00		
9	Garankuwa Zone 17	1	R 14,00	R 16,00	R 8,50	R 10,50		
10	Garankuwa Zone 2	4	R 56,00	R 64,00	R 34,00	R 42,00		
11	Garankuwa Zone 20	2	R 28,00	R 32,00	R 17,00	R 21,00		
12	Garankuwa Zone 21	2	R 28,00	R 32,00	R 17,00	R 21,00		
13	Garankuwa Zone 25	2	R 28,00	R 32,00	R 17,00	R 21,00		
14	Garankuwa Zone 3	2	R 28,00	R 32,00	R 17,00	R 21,00		
15	Garankuwa Zone 4	2	R 28,00	R 32,00	R 17,00	R 21,00		
16	Garankuwa Zone 5	1	R 14,00	R 16,00	R 8,50	R 10,50		
17	Garankuwa Zone 6	3	R 42,00	R 48,00	R 25,50	R 31,50		
18	Garankuwa Zone 7	8	R 112,00	R 128,00	R 68,00	R 84,00		
19	Garankuwa Zone 8	2	R 28,00	R 32,00	R 17,00	R 21,00		
20	Garankuwa Zone 9	2	R 28,00	R 32,00	R 17,00	R 21,00		
21	Hoekfontein	1	R 14,00	R 16,00	R 8,50	R 10,50		
22	Mmakau	2	R 78,00	R 32,00	R 17,00	R 21,00		
23	Mothutlung	5	R 195,00	R 80,00	R 42,50	R 52,50		
24		**52**						
25		**Solution Table**						
26								
27	DISTRIBUTION OF PEOPLE PER SCENARIO							
28								
29	**Source / Origin**	**No. of People / Supply**	**Trip Pattern 1**	**Trip Pattern 1**	**Trip Pattern 1**	**Trip Pattern 1**	**Total number of people**	**Cost**
30	Barseba	1	0	0	0	0	0	R -
31	Garankuwa View	3	3	0	0	0	3	R 42,00
32	Garankuwa Zone 1	3	0	0	3	0	3	R 25,50
33	Garankuwa Zone 16	6	0	0	6	0	6	R 51,00
34	Garankuwa Zone 17	1	1	0	0	0	1	R 14,00
35	Garankuwa Zone 2	4	0	0	4	0	4	R 34,00
36	Garankuwa Zone 20	2	2	0	0	0	2	R 28,00
37	Garankuwa Zone 21	2	2	0	0	0	2	R 28,00
38	Garankuwa Zone 25	2	2	0	0	0	2	R 28,00
39	Garankuwa Zone 3	2	0	0	2	0	2	R 17,00
40	Garankuwa Zone 4	2	0	0	2	0	2	R 17,00
41	Garankuwa Zone 5	1	0	0	1	0	1	R 8,50
42	Garankuwa Zone 6	3	0	0	3	0	3	R 25,50
43	Garankuwa Zone 7	8	8	0	0	0	8	R 112,00
44	Garankuwa Zone 8	2	2	0	0	0	2	R 28,00
45	Garankuwa Zone 9	2	2	0	0	0	2	R 28,00
46	Hoekfontein	1	0	0	1	0	1	R 8,50
47	Mmakau	2	2	0	0	0	2	R 78,00
48	Mothutlung	5	5	0	0	0	5	R 195,00
49		**52**	**29**	**0**	**22**	**0**	51	R 768,00

Next to columns E to G, was the insertion of extra columns having simple formula for the determination of trips which were viable and having constraint of 5km distance as maximum distance to cycle as shown in columns K to M (Table III). Column K shows the formula "IF (G3<5,1,0)", which simply implies that if the distance in cell G3 is less than 5km, the result is 1, otherwise the result is 0. The output from k is multiplied by the cells with the number of employees from each zone of origin. The solver provides that corresponding cell in the solution table should be equal or lesser than the product. Therefore, if the trip pattern is not possible, a zero is allocated to cells in column K to M and the product is as well equal to zero as shown in Table III.

A simple equation was used to determine whether any among the trip patterns would be possible with the trip duration constraint. This was achieved by adding columns for all the trip patterns and showing their overall trip durations (columns O, P, Q and R in Table IV). Other columns were inserted next to columns O to R with simple formula for the determination of how the trips were in line with the constraint of trip duration. In columns S to V of Table IV, a rule was applied. For column S, the formula "IF(O3<60,1,0))" implies that if the time for the trip in cell O3 is not up to one hour, the result is 1, otherwise the result is 0. The result is then multiplied by the cells which have the number of employees from each unit. The corresponding cell in the table of solution should not exceed the product. When the option is not achievable, zero is allocated to cells in columns S to V and the product of the multiplication of zero with zero equals zero (Table IV).

The non-negativity constriction was added through an option in the solver that may or may not be selected, by checking a box to *"Make Unconstraint Variables Non-Negative", as* reflected in figure 1.

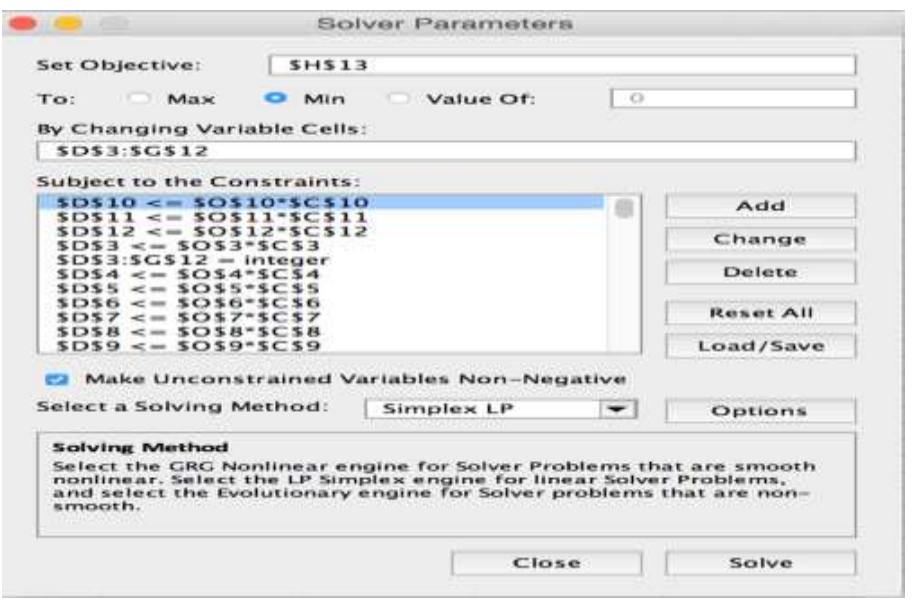

Figure 1: Excel Solver extract for ease of reference (Non- negativity constraint)

Table III: Extract of Cycling distance constraint

A	B	C	D	E	F	G	K	L	M
1		CYCLING DISTANCE					5	5	5
2	AREA	No. of People	Trip Pattern 1	Trip Pattern 1	Trip Pattern 1	Trip Pattern 1	Trip Pattern 2 Possible	Trip Pattern 3 Possible	Trip Pattern 4 Possible
3	Barseba	1	n/a	64	35	35	0	0	0
4	Garankuwa View	3	n/a	10,6	10,5	10,5	0	0	0
5	Garankuwa Zone 1	3	n/a	3	1,1	1,1	1	1	1
6	Garankuwa Zone 16	6	n/a	4,7	4,4	4,4	1	1	1
7	Garankuwa Zone 17	1	n/a	6,7	6,6	6,6	0	0	0
8	Garankuwa Zone 2	4	n/a	1,5	2,6	2,6	1	1	1
9	Garankuwa Zone 20	2	n/a	7	6,8	6,8	0	0	0
10	Garankuwa Zone 21	2	n/a	5,8	7,1	7,1	0	0	0
11	Garankuwa Zone 25	2	n/a	7,5	7,4	7,4	0	0	0

TABLE IV: TRIP DURATION DISTANCE CONSTRAINT

	A	B	O	P	Q	R	S	T	U	V
1	ORIGIN AREA	No. of People	TOTAL DURATION (MINUTES)				Trip duration constraint possible? 1=Yes, 0=No			
2			Trip Pattern 1	Trip Pattern 1	Trip Pattern 1	Trip Pattern 1	Trip Pattern 1 Possible	Trip Pattern 2 Possible	Trip Pattern 3 Possible	Trip Pattern 4 Possible
3	Barseba	1	79	276	195	188	0	0	0	0
4	Garankuwa View	3	44	63	72	65	1	0	0	0
5	Garankuwa Zone 1	3	31	32	34	27	1	1	1	1
6	Garankuwa Zone 16	6	35	39	48	40	1	1	1	1
7	Garankuwa Zone 17	1	39	47	56	49	1	1	1	1
8	Garankuwa Zone 2	4	28	26	37	29	1	1	1	1
9	Garankuwa Zone 20	2	39	48	57	50	1	1	1	1
10	Garankuwa Zone 21	2	37	43	58	51	1	1	1	1
11	Garankuwa Zone 25	2	40	50	60	52	1	1	1	1
12	Garankuwa Zone 3	2	32	34	48	41	1	1	1	1
13	Garankuwa Zone 4	2	33	35	44	37	1	1	1	1
14	Garankuwa Zone 5	1	31	31	43	36	1	1	1	1
15	Garankuwa Zone 6	3	29	28	39	31	1	1	1	1
16	Garankuwa Zone 7	8	38	47	61	54	1	1	0	1
17	Garankuwa Zone 8	2	40	49	64	57	1	1	0	1
18	Garankuwa Zone 9	2	39	47	62	54	1	1	0	1
19	Hoekfontein	1	33	37	40	33	1	1	1	1
20	Mmakau	2	48	71	60	53	1	0	0	1
21	Mothutlung	5	50	74	65	58	1	0	0	1
22		52								

The Solver calculations as contained in cell H49 of Table II were set up to reduce the cost of trip, with the application of simplex technique, a linear programming method, where the changing variable cells C30 to F48 are subjected to the constrictions as expressed earlier. The actual values of X_{ij} decision variables are embedded in the cells (C30:F48). The optimized output obtained from the simplex technique was derived in the solution cells and the associated cost was derived from cell H49 in Table II.

The solver has limitation in solving problems with fewer than 200 variables and 100 constrictions, therefore the problem was separated into two, but the outputs were combined to reliably and accurately get similar results with Solver in the excel spreadsheet as if the whole dataset were used together, without a split for all the trip origins and patterns.

The data collected and summarized in Tables V and VI were used for the optimization of the overall trip costs.

TABLE V: SUMMARY OF DIFFERENT TRIP PATTERNS DATA

Trip pattern	Average Distance	Average Duration	Total Cost
Trip pattern 1	18 km	39 minutes	R 938.00
Trip pattern 2	17 km	57 minutes	R 832.00
Trip pattern 3	20 km	60 minutes	R 444.00
Trip pattern 4	20 km	53 minutes	R 548.00

TABLE VI: TRANSPORTATION DATA FOR WORKERS RESIDING IN GA-RANKUWA

Zone of Origin	**Number of Employees**	**Trip pattern 1**		**Trip pattern 2**		**Trip pattern 3**		**Trip pattern 4**	
		**Cost	*Time	**Cost	*Time	**Cost	*Time	**Cost	*Time
Barseba	1	49.00	79	16.00	276	8.50	195	12.5	188
Garankuwa Unit 1	3	14.00	31	16.00	32	6.50	34	10.5	27
Garankuwa Unit 16	6	14.00	35	16.00	39	6.50	48	10.5	40
Garankuwa Unit 17	1	14.00	39	16.00	47	6.50	56	10.5	49
Garankuwa Unit 2	4	14.00	28	16.00	26	6.50	37	10.5	29
Garankuwa Unit 20	2	14.00	39	16.00	48	6.50	57	10.5	50
Garankuwa Unit 21	2	14.00	37	16.00	43	6.50	58	10.5	51
Garankuwa Unit 25	2	14.00	40	16.00	50	6.50	60	10.5	52
Garankuwa Unit 3	2	14.00	32	16.00	34	6.50	48	10.5	41
Garankuwa Unit 4	2	14.00	33	16.00	35	6.50	44	10.5	37
Garankuwa Unit 5	1	14.00	31	16.00	31	6.50	43	10.5	36
Garankuwa Unit 6	3	14.00	29	16.00	28	6.50	39	10.5	31
Garankuwa Unit 7	8	14.00	38	16.00	47	6.50	61	10.5	54
Garankuwa Unit 8	2	14.00	40	16.00	49	6.50	64	10.5	57
Garankuwa Unit 9	2	14.00	39	16.00	47	6.50	62	10.5	54
Garankuwa View	3	14.00	44	16.00	63	6.50	72	10.5	65
Hoekfontein	1	14.00	33	16.00	37	6.50	40	10.5	33
Mmakau	2	39.00	48	16.00	71	6.50	60	10.5	53
Mothutlung	5	39.00	50	16.00	74	6.50	65	10.5	58
***TOTAL	52	938.00		832.00		444.00		548.00	

* Duration is in minutes
** Cost is in South African Rand and it is cost per person
*** Total cost for all 52 employees

The overall cost of the subsisting single trip of all the employees of BMW residing in Ga-Rankuwa and nearby is R938.00. Trip pattern 1 costs R832, trip pattern 2 costs R444.00 and trip pattern 3 costs R548.00. The study objective

was to investigate an optimized integration of transportation modes for trips between Rosslyn and Ga-Rankuwa by BMW workers, in order to reduce the time and cost of travel. The safety and economy of the trip was also taken into consideration.

Table VII: Result of the Sensitivity Analysis

Constraints (minutes and kilometers)	Total number of workers	TP 1	TP 2	TP 3	TP 4	COST
80 min. & 2.5 km	52	35	0	10	7	R 683.50
80 min. & 5.0 km	52	23	0	29	0	R 603.50
80 min. & 7.5 km	52	16	0	36	0	R 565.00
60 min. & 2.5 km	51	41	0	3	7	R 848.00
60 min. & 5.0 km	51	29	0	22	0	R 768.00
60 min. & 7.5 km	51	15	0	29	7	R 530.00

An optimized solution was derived with the excel solver. The outcome was that 29 employees will continue to use the subsisting trip pattern (trip pattern 1, using taxis to get to work). 22 employees can use trip pattern 3 which is involves cycling to the nearest rail station; transfer from bicycle to train; boarding train and alighting at Rosslyn rail station and eventually walking to BMW gate 2. Though trip pattern 1 (initial trip) costs R938 to sojourn between Ga-Rankuwa and Rosslyn, trip pattern 3 costs R768 which is a reduction of 18% of the cost for trip pattern 1.

The analysis showed that sixty minute constraint cannot be achieved by all the trip patterns because the trip duration from Barseba to Rosslyn cannot be lesser than 79 minutes. The trip duration was increased to 80 minutes and all the requirements were satisfied though other trip durations were achievable in one hour. The optimized solution was however to maintain a maximum cycling distance of 5km while the trip duration was increased to 80 minutes. This gave an outcome that 23 employees of BMW will be moved using trip pattern 1 while 29 BMW employers will use trip pattern 3.

When trip duration and cycling distance constrictions were adjusted, the optimization of the outcome was achieved. By halving the cycling distances, the trip cost increased by 10%. This increase can greatly be attributed to cycling being viable only to 10 people as against 22, when the cycling distance was 5km. When the cycling distance was increased by half (50%) to give a cycling distance of 7.5 km, the trip cost was reduced by 31%. The reduction was as a result of cycling being applicable to 36 people as against 22 when the cycling distance was 5 km.

The result of the sensitivity analyses conducted to reduce and decrease cycling distance is presented in Table VI.

4. Results and Discussion

The average of the trip distances is 18km, the average of the trip durations is 39 minutes respectively and the average of the trip cost is R18.47.

Moving in taxi for a period of 35 minutes costs R14.00. By undertaking a trip with an integration of cycling and train a cost of R16.50 was incurred for a trip of 33 minutes. There is an extra service charge of R10.00 for taking bicycle into the train. For both trips, an average distance of 15km was travelled. Though the optimal solution has a cost implication of R603.50, the optimization gave a 36% discount when compared with the current cost of R 938.00. The implication is that integration of NMT as feeder mode enhances reduction of the transportation cost. The implication of the use of cycling is that when trip distance increases the cost of travel reduces.

Therefore, implementation of cycling into the transportation scheme is a viable option to many workers as the overall transportation cost will be reduced. In other words, cycling offers a cheaper and sustainable transportation system. This outcome is similar to the findings of Rahul and Verma (2014) that NMT contributed to the sustainability of the transportation system in India. A daily savings of $2,626 was made when cycling or walking was used to cover 1% of the trips, covered by buses and taxis, with distances that are lesser than 5km.

This research offers that the best situation is one where 56% of commuters adopts trip pattern 3 while the remaining 44% commuters continue with trip pattern 1 (Figure 2). Table VI presents the trip duration and the trip cost for each of the trip patterns. The trip cost was inclusive of the cost of the overall legs or divisions of each trip patterns. It can be obtained from table VI that by comparison, trip pattern 1 and trip 2 have higher trip costs but trip pattern 3 and 4 have lesser trip costs. The analysis in table VI also showed that longer trips attract higher cost while shorter trips attracts low cost as Barseba and Rosslyn have higher trip costs than the cost of other locations with shorter distances in Tshwane.

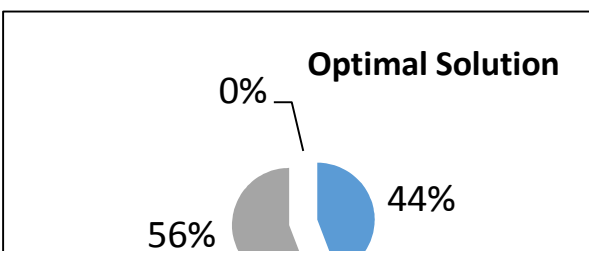

Figure 2: Optimal Solution

5. Conclusion

Integration of the non-motorized transport (NMT) like walking and cycling as feeder mode of transport will open opportunities in the transportation sector as other means of transportation from the combustion of the automobile engines would be used thereby preserving the environment from the danger of climate change. Three other trip patterns were introduced in order to study the effect of the NMT, as a feeder mode, on the trip distance and trip time. The study showed that NMT can be a

good alternative for taxis, bus and trains as feeder modes in the transportation sector. The 60 minutes duration constraint cannot be achieved because the trip time for the journey between Barseba and Rosslyn is 79 minutes which is more than the limitation of the time constraint. From the foregoing, the most applicable, acceptable and practical solution to the transportation problem under consideration is that 29 out of the 52 employees make use of trip pattern 3 for daily trip to and from work while 23 out of the 52 employees continue to use trip pattern 1. By the implementation of NMT (walking and bicycling) the trip cost would be reduced by 36%. When the above recommendation of trip pattern 3 is used for the 29 employees, a cheap, environmental friendly and sustainable transportation will be achieved.

This research work showed that implementation of cycling is viable and many people can afford and conform to it because it is a cheaper and sustainable transportation means. It is also recommended that similar work be carried out on a larger scale to improve the transportation system and increase knowledge thereby integrating cycling, a non-motorized transportation mode as a feeder mode for the motorized transportation system in other industrial areas of Tshwane and beyond (Jantjies et al. 2016).

Reference

Arora, J.S. 2012. Chapter 6: Optimum design with excel solver. Introduction to optimum design, 3: 213-273.

Beatley, T. (1995). Planning and Sustainability: The Elements of a New Paradigm. Journal of Planning Literature, 9(4): 383-395.

City of Johannesburg. (2009). Framework for Non-motorized Transport.

City of Tshwane. (2007). Integrated Transport Plan 2006-2011.

City of Tshwane. 2013. Daft 2013/14 IDP Review.

Department of Transport. (2008). Republic of South Africa, Draft National Non-motorized Transport Policy, Dec 2008.

Department of Transport: 2003. Pedestrian and Bicycle Facility Guidelines: Draft.

Department of Transport: 2014. NMT Facility Guidelines: Policy and Legislation, Planning, Design and Operations.

European Conference of Ministers of Transport. (2004). Policy Note and Declaration on Security and Terrorism in the Transport Sector, CEMT/CM (2004)5/Final

Guitink, P., Holste, S. & Lebo, J. (1994). Non-Motorized Transport: Confronting poverty through affordable mobility [online]. Available from: siteresources.worldbank.org/INTURBANTRANSPORT/T-UT-4 [accessed: 28/02/2012].

Ison, S. & Ryley, T. (2007). Options for sustainable mobility. Engineering

sustainability, 160 (1), March: 27-33.

Rahul, T.M & Verma, A. 2014. A study of acceptable trip distances using walking and cycling in Bangalore. Journal of Transport Geography, 38, June: 106-113.

Tirachini, A & Hensher, D.A. (2012). Multimodal Transport Pricing: First Best, Second Best and Extensions to Non-motorized Transport. Transport Reviews, 32 (2): 181-202.

Unep Transport Unit. (2004). Share the Road: Design Guidelines for Non-Motorized Transport in Africa.

Victoria Transport Policy Institute. (2012). TDM Encyclopedia: Evaluating Non-Motorized Transport [online]. Available from: www.vtpi.org/tdm/tdm25.htm [accessed: 08/01/2013].

Jantjies, M., Ndambuki, J.M., Kupolati, K.W., Adeboje, A.O. & Kambole, C. (2016). Reduction of Traffic Congestion and Carbon Emissions through Park and Ride Transportation System. *Proceedings of 3rd International Conference on African Development Issues.* (pp. 275 – 280). CU-ICADI.

\

Covenant Journal of Informatics & Communication Technology. Vol. 5 No. 1, June, 2017

An Open Access Journal available online

Ameliorating Traffic Congestion and Impact on Climate Change with Park and Ride Transport

Jacqueline Rikhotso[1], Julius Ndambuki[2] Williams Kupolati[3], Adeyemi Adeboje[4] & Chewe Kambole[5]

[1]Department of Civil Engineering,
Tshwane University of Technology, Pretoria, South Africa
tintswaloj@gmail.com
[2]Department of Civil Engineering,
Tshwane University of Technology, Pretoria, South Africa
NdambukiJM@tut.ac.za
[3]Department of Civil Engineering,
Tshwane University of Technology, Pretoria, South Africa
KupolatiWK@tut.ac.za
[4]Department of Civil Engineering,
Tshwane University of Technology, Pretoria, South Africa
AdebojeAO@tut.ac.za
[5]Department of Civil Engineering,
Tshwane University of Technology, Pretoria, South Africa
KamboleC@tut.ac.za

Abstract: Traffic congestion occur as more vehicles ply the road and result in reduced travel speed, increased travel time, unnecessary queuing, obstruction on travel path and impediment to traffic flow. Thirteen per cent of greenhouse gases (GHG) emitted are caused by the transportation system which continues to grow. Fume emanating from vehicles contributes greatly to the emission of GHG. Park and Ride was investigated within the Central Business District (CBD) of Tshwane with a view to improving the traffic congestion and reducing the effects of GHG on the climate. Traffic counts and questionnaires distribution were done on the major access routes to the CBD. The quantities of carbon dioxide (CO_2) emitted by traffic and that would be reduced when park and ride system is implemented in the City of Tshwane Metropolitan Municipality (CTMM) were determined. Results of traffic volume counts showed high dependence of more

than 70% of people on passenger cars as the mode of transit within the study area. It also revealed that almost 89% of the interviewed population are delayed by traffic, on their way to the work place in the morning. Fifty-four per cent of the people interviewed showed readiness to utilize the park and ride facility if their safety and security would be guaranteed. Furthermore the study showed that 96.2% of CO_2 emitted could be reduced by the implementation of the park and ride system on the A Re Yeng BRT and also in the major cities of Tshwane.

Keywords: Greenhouse gases, traffic congestion, traffic flow, traffic volume, travel speed.

1. Introduction

Traffic congestion is usually experienced when heavy traffic is attracted to or generated from towns and central business districts (CBD), due to day-to-day activities of people and struggle for survival. It also leads to high energy consumption, causing high carbon-monoxide (CO) emissions from internal combustion of automobile engines. Carbon monoxide a colourless, odourless, tasteless but toxic gas poisons the lungs of human beings when inhaled through breathing mechanism and displaces oxygen from the blood stream. The normal supply of oxygen is truncated and the heart functions at great risk (Carbon Monoxide, 2011).

Increase in vehicular traffic causes reduced speed of movement, queuing, and delayed arrival time. The aforementioned phenomena characterize traffic congestion. Great energy is utilized or used up in traffic congestion. This results in emission of great quantum of carbon monoxide (CO) due to combustion of fuels by the engine of automobiles. Carbon dioxide (CO_2) results from the burning of carbon monoxide (CO) in the presence of oxygen (Carbon Monoxide, 2011).

Traffic congestions causes variation in vehicular speeds and enhances the emission of CO_2 (Barth & Boriboonsomsin, 2010). The Republic of South Africa is listed among the twenty leading countries generating greenhouse gases emission in the world (Energy Information Agency, 2010). Interestingly, the combustion of petrol and diesel of automobiles, in the transportation sector, emits great quantum of greenhouse gases (Department of Environmental Affairs, 2010). Traffic congestion and the attendant emission of CO_2 could be reduced when park and ride transportation system, a modest traffic solution, is implemented (Spillar, 1997). Park and ride is a convenient system which allows vehicular parking out of the city. Such parking lots are integrated to the existing transportation system in the CBD (Lam et al. 2007).

Park and ride facility can also be called intermodal transportation scheme. The duties of the park and ride scheme changes swiftly with changes in traffic conditions (Spillar, 1997). Park and ride schemes are designed to eliminate congestion in urban areas with high traffic demands. Cities, towns and locations are connected with the provision of parking areas for the convenience of movements to important locations such as airports, amusement

parks, recreation centers, shopping malls and stadia. High occupancy vehicles (HOV), public transport developments and ride sharing are proximate to park and ride facilities (Vincent & Hamilton, 2007).

The land use, location, population and work force of a particular area dictate the efficiency of the park and ride scheme (De Aragon, 2004).

According to De Aragon (2004). Park and ride schemes are classified by the functions they serve in the different locations where they are utilized. They can be generally described as follows:

- Remote – This is usually located at a far distance from major areas and residences. They are usually in rural communities.
- Suburban – This is situated near the outer edges of urban areas. Here the private vehicles are dominant while public modes of transportation such as rails, ferries and buses are mainly used to collect and distribute passengers.
- Local – This may be located along or near the end of a main transit. There is no provision for special or dedicated service, hence it is served by existing roads. The transit level may be low.
- Peripheral – This is situated at the CBD's edge or at areas where major events take place. Its main role is to enhance more parking by diverting commuters from entering areas that are congested and connecting them to large expanse of land in areas with free or cheap parking facilities.

Park and ride facilities are described by Spillar (1997) as follows:

- Informal – This is a simple and regular transit for commuters to park and access nearby streets or adjacent properties with ease and convenience.
- Exclusive – This is designed and constructed to serve the operation of the park and ride scheme. It is famous in urban areas with different modes of transportation such as taxis, buses, BRTs and rails
- Shared-use – This has multiple functions like parking site for private and commercial uses for schools, churches, communities and groups in smaller urban areas with less demands. It can be implemented within short time, it has low maintenance cost resulting from its low capacity.

The transportation means for the study area was grouped as 35% mobility, 35% private and 30% public facilities (Tshwane Integrated Development Plan, 2006). Private transportation is the most convenient transportation means and is on the increase. Its increase has continuously led to increase in accident and traffic congestion in the CBD, especially at peak periods. Increase in the number of private vehicles is however not sustainable in the CBD of Tshwane (Tshwane Integrated Development Plan, 2006).

Tremendous efforts had been made to ameliorate traffic congestion and improve the transportation system in Tshwane by integrating private and public, motorized and non-motorized transportation systems in order to achieve accessible, safe, secured and economic transportation with time gain

(City of Tshwane Comprehensive Integrated Transport Plan, 2015).

The main aim of this work is to ameliorate the traffic congestion and the resulting greenhouse gases emitted, thereby reducing their effects on the climate change in the City of Tshwane. This will guaranty a safe, healthy and convenient environment through the implementation of park and ride scheme.

This work is an extension of (Rikhotso et al., 2016). The abstracts, main body and results had been extensively revised.

2. Study Area and Methods

Tshwane region, a cosmopolitan city in Gauteng province of South Africa was the study area for this research. Tshwane is the capital and also the largest metropolitan municipality of the Republic of South Africa.

Secondary data were sourced from the agencies of government. Structured questionnaire was distributed to people in the study area.

The specific methods used for the research are:

i. GIS data to generate orthor-photos.
ii. Traffic counts.
iii. Questionnaire method
iv. Determination of Carbon emitted from Sale and consumption of fuel.

Secondary data were sourced from the agencies of government. Structured questionnaire was distributed to people in the study area. The data collected for the work are as follow:

i.Geographic Information Systems (GIS) generated Ortho-photos: Data for the roads and storm water were retrieved from the division of infrastructure technology information management of the CTMM. The data were developed with the use of GIS. Ortho-photos were viewed using the MrSID viewer program as presented in the Tshwane municipality map in figure 1.

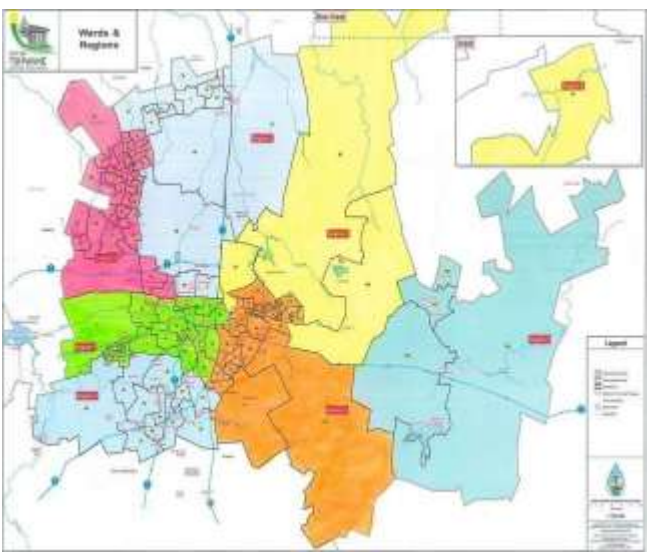

Figure 1: Map of the Metropolitan Municipality of the City of Tshwane.

ii. Traffic Counts: Data on 12 hour traffic volume were obtained from manual traffic counts conducted between 6am and 6pm at the four main access roads to the CBD of Tshwane as recommended by (Highway Capacity Manual, 2000). Traffic count was conducted from Monday, March 5 to Friday, March 9, 2012. The traffic count method used for enumerating automobiles was the classified count. It was conducted on Nelson Mandela, Struben, Pretorious and Paul Kruger Streets.

Observations were made on the turning of the vehicles at intersections on DF Malan and Struben Streets; Boom and Paul Kruger streets; Hamilton and Pretorius streets and Willow and Nelson Mandela Streets.

iii. Questionnaires: A set of well-structured questionnaire having eleven questions was rated and distributed to 318 respondents in the BCD of Tshwane between Monday and Friday.

The questionnaire had multi-choice answers for respondents to choose their answers against each of the questions asked.

The structured questions are summarized as follows:

1. Place of residence?
2. Nature of work or profession?
3. Transport mode used from home to work?
4. Work distance from home?
5. Trip time from home to work?
6. Are you held in traffic from home to work?
7. If answer to question 6 is yes, how frequent?
8. How much fuel will you use if you are going to work from home in your private vehicle?
9. Do you move alone or with friends, neighbor of family when you travel in your private vehicle?
10. If there is an improvement that will guarantee safety, reliability, efficiency and economy of the public transport, will you drop your private vehicle for the public vehicle? Are you aware that patronage of the public transport will enhance the reduction of the carbon emitted in the environment?
11. Will you park your private vehicle at a dedicated and safe place if there is provision of convenient, easy, cheap, reliable and safe public means of transportation from your home to work?

iv. Determination of Carbon emitted from Sale and Consumption of Fuel: The volume of fuel sold was obtained from department of energy of CTMM. The equivalence of the volume of carborn dioxide emitted was obtained from the relationship shown in equation (1).

$$MtCO_{2e} = \sum(f_p * EF_p) + (f_d * EF_d) \quad (1)$$

where:

f_p = *petrol volume*

EF_p = *factor for petrol emission*

F_d = *diesel volume*

EF_d = *factor for diesel emission*

$MtCO_{2e}$ = *Equivalence of Carbon di Oxide in Mega Tonnes*

The quantity of CO_2 obtained from the combustion of a litre of petrol or diesel is dependent on an equivalence of chemical constituents of either the petrol or diesel. The assumption is that the equivalence for petrol is 2.36 of CO_{2e} while that of diesel is 2.60kg of CO_{2e} (Climate leaders greenhouse gas inventory protocol, 2008).

The values were used to determine the total volume of Co_2 emitted from petrol and diesel. Though nitrous oxide (NO_2) and methane (NH_4) are also gases that emit greenhouse effects, they were not

used in the determination of carbon emitted.

3. Discussion of Results

3.1 Layout Plan for Park and Ride Transportation Scheme

Figure 2 presents the Are Yeng BRT routes utilized to generate the layout plan for the transportation scheme. The Are Yeng transportation route is direct, accessible and connects different areas with great importance because of the good level of service its dedicated lanes provides for safe, easy and convenient transit from its routes to park and ride facilities (De Aragon, 2004).

Lands identified for the implementation of park and ride scheme are lands adjacent to the existing or proposed A Re Yeng BRT route; vacant sites on the main roads of Tshwane; rezoning or expropriation for land ownership or acquisition and also effects of the public transportation system on existing traffic records.

Fallow plots of land available for park and ride facilities are shown in table I. The nearness and adequacy of the plots of land identified for use as park and ride transportation schemes are shown in table II.

AVAILABLE SPACE FOR PARK AND RIDE FACILITY

Space	**Area located**	**Proprietor**	**Accession**	**Along BRT lane**	**Impacts Traffic**
Vlakfontein 329JR	Mamelodi	CTMM	Assigned	*	*
Ombre 636JR	Paul Kruger Str.	CTMM	Assigned	*	*
Klipkruisfontein	Soshanguve	CTMM	Assigned	*	*
Ext 507, Erf 394	Wonderpark	Private	Seizure	*	*
Wonderboom	Annlin	Private	Seizure	*	*

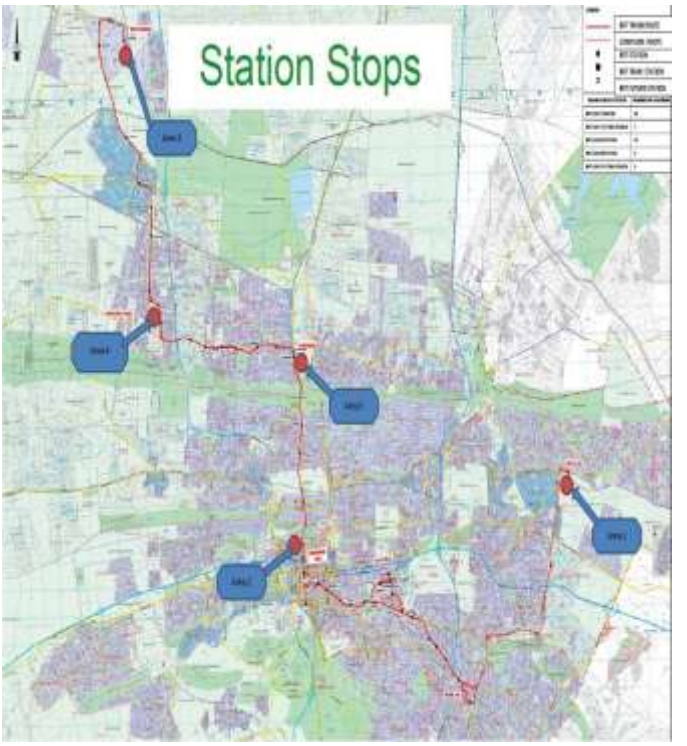

Figure 2: Map of the City of Tshwane Metropolitan Municipality

TABLE II: DISTANCE BETWEEN LOCATIONS AND CBD

Area	**Distance from designated area to CBD**
Area 1	17 km
Area 2	3 km
Area 3	26 km
Area 4	16 km
Area 5	7.5 km

3.2. Estimation of Carbon Emissions

The fuel consumption for private vehicle car per 100km is 14.71 and 8.241 for congested and unrestricted traffics respectively (Treiber et al. 2007).

Volvo bus (2013) showed that the rate of fuel consumption for bus per 100km is 26 litres when the bus is moving averagely at a speed of 60km/h. The above assumption that a vehicle or private car consumes 8.241 litres of fuel

to cover a distance of 100km when the traffic is unrestricted and 14.71 litres of fuel to cover the same distance when the traffic is congested was used in the design of Traffic flow in the Tshwane region.

The combustion rate of 8.241 litres of fuel was taken for the 100km in the first segment of the trip while the combustion rate of 14.71 litres of fuel was utilized for the 100km in the second segment of the journey in the morning. The reverse was utilized for the trips in the afternoon. To determine the quantity of emitted carbon per litre of fuel, the average value of the emission of petrol and the average value of the emission of diesel were used. Therefore the fuel emission factor used for the calculation of carbon emitted by vehicle both leaving and entering Tshwane is 2.48kg$CO_{2e.}$ The capacity of the facility was determined by the available spaces. While the park and ride facilities were assumed as operating at full capacity, the capacity of a passenger bus was taken as 65.

The emission factor used for buses was 2.6kgCO_{2e} and the fuel consumption rate of 26 litres was projected to be consumed by the bus for a distance of 100 km when the traffic flow is unrestricted. It was assumed that the consumption factor of the bus rapid transit would be constant as the bus would be travelling on its dedicated lane. Data of the air pollution within the city of Tshwane was given by the department of energy of the Tshwane region. The quantities of estimated carbon emission for Tshwane and the Republic of South Africa from year 2005 to 2014 are presented in tables III and IV respectively. There is a substantial increase in the greenhouse gases emitted as presented in figure 3.

The records of the fuel volume sale and consumption data in 2014 shows that the contribution of the city of Tshwane is 4.439 MtCO2e out of South Africa's 61.009 MtCO2e of carbon emission which is 7.2% (City of Tshwane greenhouse gas inventory, 2014).

From 2011 to 2013 the city of Tshwane emitted 13.180 MtCO2e. In 2012 the greatest contributor of the greenhouse gas emission then was from industrial pollution which produced 4.100 MtCO2e, which was 31.11% of the overall greenhouse gas emissions. The transportation sector was the next (second) contributor of greenhouse gas emission after the industrial pollution. The transportation sector contributed 4.061 MtCO2e which was 30.82% of the entire emissions of greenhouse gas (City of Tshwane greenhouse gas inventory, 2014). The numerical values of the emission of carbon for year 2013 slightly exceeded that of 2012 as the city of Tshwane produced 4.366 MtCO2e as shown in table III.

The estimated quantity of carbon emitted by cars is presented in table V while the estimated quantity of carbon emitted by buses is presented in table VI. Without recourse to the difference in the travel speeds of car and bus, the two vehicles will travel the same distance from one point to the other but their speed, rate of fuel combustion and the resulting carbon emission differ.

Assuming all the car users shown in Table V uses the park and ride facilities for their journey within Tshwane region of the Republic of South Africa and

move to the central business district (CBD) by public buses, 96.2% of the estimated carbon emitted in the region of Tshwane would be prevented.

A standard bus does not take much space on the highway and does not cause hectic traffic and congestion on the highway. The dimension and shape of buses are moderate, they are not heavy and can be easily manoeuvred. Buses may enhance convenient, smooth and quick responses to changing or prevailing circumstances or demands without requiring for special infrastructures (Chapman, 2007).

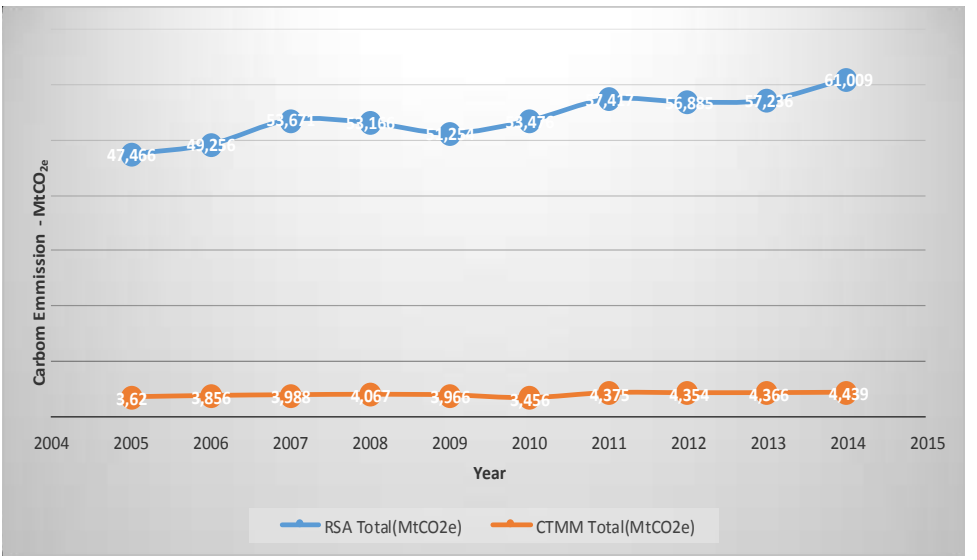

Figure 3: Carbon emission estimated from RSA and CTMM Annual Fuel Sales volumes and consumption

TABLE III: EMITTED CARBON FOR TSHWANE CITY FROM ANNUAL SALE OF FUEL FROM 2005 TO 2014

Year	Diesel (litre)	Petrol (litre)	Carbon produced from Diesel (kg of CO_{2e})	Carbon produced from Petrol (kg of CO_{2e})	Total Carbon produced from Diesel (kg of Co_{2e})	Total Carbon produced from Petrol (kg of Co_{2e})	Total Carbon produced ($MtCO_{2e}$)
2005	455 128374	1 032 522 138	1 183 333 772	2 436 752 245.68	3 620 086 018	3 620 086.018	3.620
2006	537 571 166	1 041 667 593	1 397 685 032	2 458 335 519.48	3 856 020 551	3 856 020.551	3.856
2007	583 543 659	1 047 123 983	1 517 213 513	2 471 212 599.88	3 988 426 113	3 856 020.551	3.998
2008	653 686 754	1 003 270 446	1 699 585 560	2 367 718 252.56	4 067 303 813	4 067 303.813	4.067
2009	597 929 385	1 021 620 026	1 554 616 401	2 411 023 261.36	3 965 639 662	3 965 639.662	3.966
2010	564 580 485	842 620 954	1 467 909 261	988 585 451.44	3 456 494 712	3 456 494.712	3.456
2011	724 834 772	1 055 244 617	1 884 570 407	2 490 377 296.12	4 374 947 703	4 374 947.703	4.375
2012	740 176 729	1 029 548 505	1 924 459 495	2 429 734 471.80	4 354 193 967	4 354 193.967	4.354
2013	753 757 478	993 799 248	2 020 522 296	2 345 366 225.28	4 365 888 521	4 365 888.531	4.366
2014	777 123 960	1 024 607 025	2 020 522 296	2 418 072 578.26	4 438 594 874	4 438 594.874	4.439

TABLE IV: EMITTED CARBON FOR THE REPUBLIC OF SOUTH AFRICA FROM ANNUAL SALE OF FUEL FROM 2005 TO 2014

Year	Diesel (litre)	Petrol (litre)	Carbon produced from Diesel (kg of CO_{2e})	Carbon produced from Petrol (kg of CO_{2e})	Total Carbon produced from Diesel (kg of Co_{2e})	Total Carbon produced from Petrol (kg of Co_{2e})	Total Carbon produced ($MtCO_{2e}$)
2005	8 116 573 441	11 170 710 222	21 103 090 946.60	26 362 876 123.92	47 465 967 070.52	47 465 967.07052	47.466
2006	8 707 405 264	11 278 412 253	22 639 253 686.40	26 617 052 917.08	49 256 306 603.48	49 256 306.60348	49.256
2007	10 141 584 286	11 568 813 336	26 368 119 143.60	27 302 399 472.96	53 670 518 616.56	53 670 518.61656	53.671
2008	10 385 030 955	11 086 938 407	27 001 080 483.00	26 165 174 640.52	53 166 255 123.52	53 166 255.12352	53.166
2009	9 437 131 324	11 321 186 218	24 536 541 442.40	26 717 999 474.48	51 254 540 916.88	51 254 540.91688	51.254
2010	10 170 466 384	11 454 711 308	26 443 212 598.40	27 033 118 686.88	53 476 331 285.28	53 476 331.28528	53.476
2011	11 224 553 285	11 963 310 914	29 183 838 541.00	28 233 413 757.04	57 417 252 298.04	57 417 252.29804	57.417
2012	11 228 716 399	11 733 080 659	29 194 662 637.40	27 690 070 355.24	56 884 732 992.64	56 884 732.99264	56.885
2013	11 890 350 007	11 152 866 181	30 914 910 018.20	26 320 764 187.16	57 235 674 205.36	57 235 674.20536	57.236
2014	13 168 816 974	11 343 566 879	34 238 924 132.40	26 770 817 834.44	61 009 741 966.84	61 009 741.96684	61.009

TABLE V: ESTIMATED CARBON EMISSION BY CARS USING PARK AND RIDE FACILITIES

Areas located	Distance from location to CBD (km)	Consumption 1^{st} segment of Journey (ℓ)	Consumption 2^{nd} segment of Journey (ℓ)	Total Journey Consumption (ℓ)	Carbon Emission Factor (kg CO_{2e})	Carbon Emission per Journey per Car (kg of CO_{2e})	Total Available Parking space	Total ($kgCO_{2e}$)	Total ($MtCO_{2e}$)
1	17	0.700	1.250	1.951	2.48	4.838	2000	9676.142	
2	3	0.124	0.221	0.344	2.48	0.854	1000	853.777	
3	26	1.071	1.912	2.984	2.48	7.399	2000	14798.905	
4	16	0.659	1.177	1.836	2.48	4.553	2000	9106.957	
5	7.5	0.309	0.552	0.861	2.48	2.134	2000	4268.886	
Total Carbon emitted in January								38704.5664	
Total Carbon emitted for the whole Journey (monthly – single trip)								774091.328	0.00077
Total Carbon emitted for the whole Journey (monthly – return trip)								1548182.656	0.0015
Total Carbon emitted for the whole Journey (annual – single trip)								9289095.936	0.009
Total Carbon emitted for the whole Journey (annual – return trip)								18578191.87	0.018

TABLE VI: ESTIMATED CARBON EMISSION BY BUSES USING PARK AND RIDE FACILITIES

Areas located	Distance from location to CBD (km)	Total Fuel consumed(ℓitre)	Carbon Emitted (kg CO_{2e})	Carbon Emission per Journey per Bus (kg CO_{2e})	Total Buses required for available space	Total ($kgCO_{2e}$)	Total ($MtCO_{2e}$)
1	17	4.400	2.60	11.492	31	353.6	
2	3	0.780	2.60	2.028	15	31.2	
3	26	6.760	2.60	17.578	31	540.8	
4	16	4.160	2.60	10.816	31	332.8	
5	7.5	1.950	2.60	5.070	31	156	
Total emission for the whole Journey						1414.400	
Total emission for the whole Journey (monthly – single trip)						18288.0	0.0000282
Total emission for the whole Journey (monthly – return trip)						56576.0	0.0000565
Total emission for the whole Journey (annual – single trip)						339456.0	0.000339
Total emission for the whole Journey (annual – return trip)						648912.0	0.000679

IV. Conclusions

This work shows that the quantity of carbon emitted, as obtained from the estimates of the fuel volume sale and consumption, in Tshwane in particular and the entire Republic of South Africa is increasing annually. The city of Tshwane in 2014 contributed 4.439 $MtCO_{2e}$ or 7.2% of South Africa's 61.009 $MtCO_{2e}$ as obtained from the records of the fuel volume sales and consumption data.

Implementation of the of park and ride facilities in the Republic of South Africa will reduce 96.2% of carbon emission by private vehicles (cars) traveling along the A Re Yeng BRT route. Buses emit only 3.8% of the total emission while the remaining emissions come from cars. Park and ride scheme may be useful in effective reduction of the problems of traffic congestion and the resulting emission of greenhouse gas which have impacted negatively on the environment in Tshwane and the entire Republic of South Africa. If implemented, park and ride will surely ameliorate the insufficient parking facilities within the City, ease traffic flow and reduce emission of carbon which negatively affects the climate.

Acknowledgement

The authors greatly acknowledge the management of Tshwane University of Technology, Pretoria, South Africa.

References

Barth, M and Boriboonsomsin, K. (2010). Real-world carbon dioxide impacts of traffic congestion. University of california transportation center uctc-fr-2010-11.

Carbon Monoxide. (2011). [Online]. Available on: http://en.wikipedia.org/wiki/Carbon_monoxide [Accessed: October 28 2011].

Chapman, L. (2007). Transport and climate change: a review. *Journal of transport geography*. Vol 15. pp 354-367.

City of Tshwane Comprehensive Integrated Transport Plan. (2015). Chapter 3: sustainable transport. Draft report.

City of Tshwane greenhouse gas inventory. (2014). An inventory of the city of Tshwane's carbon footprint of its 2012/2013 financial year (July 2012- June 2013). Final report.

Climate leaders greenhouse gas inventory protocol (2008). Direct emissions from mobile combustion sources. Design principles guidelines.

De Aragon, F. (2004). Park and Ride options for Tompkins country white paper. Ithaca-tompkins country transportation council.

Department of Environmental Affairs. (2010). South Africa. National Climate Change response green paper. Pp 6-38.

Energy Information Agency. (2010). Department of Energy, South Africa. [Online]. Available on: http://www.solarpowerwindenergy.org/2010/01/24/top-20-countries-with-co2-emissions/ [accessed: October 25, 2011].

Highway Capacity Manual. (2000). *Transportation research board*, washington, d.c. *Isbn 0-309-06681-6*

Lam William, H. K., Wong, Z.C.Li.S.C. & Zhu, D.L. (2007). Modelling an

Elastic-Demand Bimodal Transport Network with Park-and-Ride trips. Vol. 12, no. 2: pp 158-166.

Rithotso, J.T., Ndambuki, J.M., Kupolati, K.W., Adeboje, A.O. & Kambole, C. (2016). Reduction of Traffic Congestion and Carbon Emissions through Park and Ride Transportation System. *Proceedings of 3rd International Conference on African Development Issues*. (pp. 275 – 280). CU-ICADI.

Spillar, R.J. (1997). Park and Ride Planning and Design Guidelines. *Monograph* 11.

Treiber, M., Kesting, A. & Thiemann, C. (2007). How much does traffic congestion increase fuel consumption and emission? Applying a fuel consumption model to the ngsim trajectory data. Submission for the annual meeting of the transportation research board 2008.

Tshwane Integrated Development Plan. (2006). Chapter 2: Situational Analysis: major features and priority development needs. First revision.

Vincent, M. & Hamilton, B.A. (2007). Park and Ride: Characteristics and Demand Forecasting. Land Transport New Zealand: *Research Report* 328.

Volvo Bus. (2013). [online] available from: http://volvobusenvironmentblog.com/2013/09/12/coach-fuel-consumption/. [Accessed: October 6 2015].

Covenant Journal of Informatics & Communication Technology. Vol. 5 No. 1, June, 2017

An Open Access Journal Available Online

Design and Implementation of a Low-Cost Low Interaction IDS/IPS System Using Virtual Honeypot Approach

Marcos Rodrigues[1] **&Olamilekan Shobayo**[2]

[1]Sheffield Hallam University, Sheffield, United Kingdom
[2]Covenant University, Ota, Nigeria
Contact(s). m.rodrigues@shu.ac.uk,
olamilekan.shobayo@covenantuniversity.edu.ng,

Abstract— Network attacks have become prominent in the modern-day web activities and the black hat community have also gain more sophistication with the tools used to penetrate poorly guarded or unguarded networks. Network security administrators have also moved swiftly to counter the threats posed by the attacker with different network intrusion detection and monitoring tools. Low interaction honeypots were developed to entice hackers without causing any serious downtime to the production network, so that their activities and the way they access the network can be studied with a minimal setup cost. In this work, a low interaction virtual honeypot using the Honeyd daemon to lure attackers to the network and alert the attacker's activities in the network using the Snort IDS. The data captured is analysed based on the protocol and port used. It is then validated by analysing the attacker's activities once it is logged and accessed through Wireshark protocol analyser.

Keywords/Index Terms—Low Interaction Honeypot, High Interaction Honeypot, Intrusion Detection and Prevention, Traffic monitoring

1. Introduction

According to the survey carried out by (Richardson, 2010), Cyber-attacks have become a pertinent issue that have cost organisations worldwide an estimated $150 million stating that much of attack targeted to organisations ranks from Malware infection 67%, Fraudulently represented as a sender of phishing mail 37%, laptop or mobile hardware theft or loss 34% and Denial of service 17%.

During the past decade, there has been numerous network security tools developed for organisations which

includes Firewalls and NIDS. Firewall for example, helps protect these organisations by preventing an attacker from gaining access to the internal network and tools such as NIDS allows organisations to detect and identify attacks, provide mechanisms that react to the detected attacks or at the barest minimum, reduces the effect of the attack. But because attackers always come with new tricks and these tools lacks the functionality of detecting or fending off the newer attacks and the collection of more information about the attacker's activities, skills and methods. For example, Signature based IDS's does not contain the attack signature of a newer attack in its signature database, therefore it will allow an attack to get through to the network if its signature is different from the one contained its database.

Nowadays, for organisations to protect their networks and build efficient security systems, it is necessary for network security system developers to gain the attackers knowledge and attack plots (Anuar, et al., 2006). Many non-profit organisations and educational institutions have spent time to research into cyber-attacks and analyse the methods and tactics used by the so-called Black hat community which act against organisations production network.

An important network tool that is used by different organisation to monitor the Black hat community is the Honeypot. According to (Provos & Holz, 2008), a honeypot is a closely monitored computing resource that we want to be probed, attacked or compromised. It is a form a decoy system that is set up to detect or confuse unauthorised attempts on information systems. Honeypots also allows us to analyse how attackers explore system and network vulnerabilities. Because honeypots have no production values it constitutes an extra cost when it is being set up in a production network because of the extra network components that is required for the setup. As suggested by (Ayeni, Alese and Omotosho 2013) Intrusion detection has become a very delicate matter over the last few years within the broad realm of network security. With so much advancement in hacking, if attackers try hard enough, they will eventually succeed in infiltrating the system. Therefore, there is a need to constantly or periodically monitor what is taking place on a system and look for suspicious behaviour. Vulnerabilities in common security components such as firewalls, security patches, access control and encryption are inevitable, so hackers take advantage of these shortcomings to infiltrate the system. (Sabah & Vandana, 2013) To reduce cost, low interaction honeypots were developed which will simulate the network components instead of incurring the cost of setting up the high interaction counterpart with lesser sophistication and richness of data as the alternative forgone. This report focuses on the low interaction technique for honeypot deployment.

2. Background and related work

Network attacks as defined by (Ghorbani, et al., 2010) “is a set of malicious activities to disrupt, deny, degrade or destroy information and service resident in computer networks”. Streaming of data through a network is the main source of attack on that

network and its aim is to disrupt the traffic going through that network and making the network vulnerable to other attacks by reducing its integrity and confidentiality. Network attacks ranges from an individual receiving an obnoxious email from another individual to attack on the components of a network, important information and critical data. Examples of attacks on computers include email viruses, worms, Trojan horses, unauthorised access, amending data on a system by taking advantage of a bug on the software. To perpetrate these attacks, the methods used by the attackers can be generalised into Masquerading, Social Engineering, Vulnerability Scanning and functionality abuse.

Social Engineering attack is used to mislead its prey by persuading them aggressively to give their authentication details (Amitabh, et al., 2004). Examples are email phishing and Trojan Horse; Masquerading attack is when the attacker poses as a legitimate user in a network to gain higher privileges than they should i.e. logging in as an administrator into a network which they are not. This is achieved by bypassing the means of authentication with stolen logon passwords and user identities; Vulnerability scanning methods are software bugs attached to a legitimate program which the attacker uses to obtain access illegally to a system. Examples include improper handling of temporary files, race conditions and buffer overflows.

In order to manage honeypot system using web interface, (Anuar, et al., 2006) created Honeyd@WEB. Through web interface, Honeyd@WEB was used to design a low-involvement (low-interaction), production, dynamic and manageable honeypot. It combines techniques such as "Deception ports" on production network to simulate honeypot services which are used in place of well-known services such as HTTP, POP, DNS and FTP and "proximity Decoys" where honeypots decoys are situated very close to the production host i.e. in the same local subnet. The main purpose of their research was to detect real systems and the Honeyd@WEB solution was deployed in the internal network to detect internal attackers.

Similarly, they also used the Honeyd@WEB to detect firewalls that are not configured properly and to detect worms and Trojans.

(Vollmer and Manic 2014), created a deceptive virtual host (low interaction honeypot) by combining 3 components namely:

- Network Entity Identification (NEI).
- Dynamic Virtual Host (DVH) configuration.
- Virtual Host Instantiation (VHI).

The NEI component is used to monitor the network traffic by extracting the source, destination and activities of each port. They evaluated tools like P0f, Ettercap, Snort, TCPdump and Ntop to provide network host identification.

The DVH component is configured using Honeyd as it provides autonomous configuration with low expenses as compared to the manual (High interaction honeypot) configuration. Its main objective is to automatically configure and update a random amount of virtual host dynamically based on the data it gathered from the actual host using Ettercap. The DVH components

was described in 4 sections namely OS selection, OS name mapping, MAC creation and Network service emulation.

The VHI and update component is used to instantiate the virtual host. They created an initial configuration file and made changes to the configuration file of the virtual host running under Honeyd while the system is running.

(Kaur and Saini 2013), created a Honeynet to analyse network traffic and prevent attacks on protocol and port basis. The Honeynet was deployed to capture keystrokes of the attacker's activities and the captured data was analysed for the purpose research.

Honeyd was used as the low interaction honeypot to create virtual host and simulate some services on them including TCP, UDP and ICMP. For the high interaction honeypot, a real host running on Windows XP SP2 operating system was used and Sebek-win-3.0.5 was also used as the data capture tool. A Honeywall is also configured in the setup with all three NIC's attached to the Honeywall system used at once. The Honeywall connected the Honeynet (Low and High interaction honeypot) and the production network in a bridge mode. This bridge mode made it very difficult for the attacker to detect the honeypot.

The Honeywall was configured not to have any IP address except for the interface connected to the management machine. This feature enables the Honeywall to appear in a stealth mode and transparently control and detect all information that moves across it. When malicious activities are detected, it is forwarded to the Honeynet machines i.e. (the Low and High interactions honeypots) and the activities are logged and the data captured are analysed.

HPing3 was used to launch attacks on the honeypots from a computer connected to the production network, the attacks launched includes: SYN flag, DoS, Smurf attack and flooding by using IP spoofing. The honeypots could capture the launched attacks and the types of attacks were shown using the Sebek software.

3. System Architecture

The architectural model of the implemented virtual honeypot network is shown in Figure 1 and it is achieved using the Honeyd software to simulate the virtual hosts that can be interactive with an attacker and used to provide arbitrary services like TCP, UDP and ICMP to deceive the attacker into thinking that it is communicating with a real computer on a real network.

Although the Honeyd software can also be configured to log the activities of the attacker, the Snort IDS/IPS software was used for the logging of these activities because it provides a more powerful analysis and signature categorisation of the attacker's activities.

Both software provides both logging and analysis characteristics and to make this work more robust, the Wireshark network protocol analyser was selected to give detail analysis of the attacker’s activities on the network by monitoring the inflow and outflow of data across the host computer on the interface connected to the internet which is also configured as the same port where the honeypot and the IDS/IPS in listening to.

The system architecture in Figure 1 shows the experimental design of the

proposed technique for the deployment of the IDS/IPS system. As seen from the diagram, the IDS system is placed behind a firewall. The firewall helps filters traffic between a protected (internal) network and an unprotected (external) network. This also helps to make the attacker thinks he is attacking a real network.

It also keeps unwanted packets from entering the protected network. Honeypots can either be placed in the front of a firewall, in the DMZ, or behind a firewall. When dealing with IDS/IPS networks, as suggested by (Annamma , et al., 2011) it is always a good practice to setup the honeypots behind the firewall to appear as a legitimate network to the intruder. Therefore, for this design, I have chosen to implement the Honeypot behind the firewall to be in accordance to industry standard and to preserve the authentication of the Honeypot concept.

3.1. Virtual Honeypot Implementation

The virtual host is used to simulate network delay and packet loss rate. The simulated network consists two virtual host and two Cisco routers. The virtual router 1running as Cisco 2600 series personality is used to separate the network 192.168.7.0/24 and the network 172.16.0.0/24. Virtual router 2 also running on the cisco 2600 personality is used to separate the network 172.16.0.0/24 and the network 172.20.0.0/24. Virtual router 1 access address is 172.16.0.1 and the virtual router 2 access address is 172.20.0.1.

The virtual host 1 in the 172.16.0.0/24 network with the IP address 172.16.0.2/24, running on the Linux 2.6.20-1 as the personality, while the virtual host 2 is on the network 172.20.0.0/24 network with the IP address 172.20.0.2/24 and running Windows XP professional as its personality.

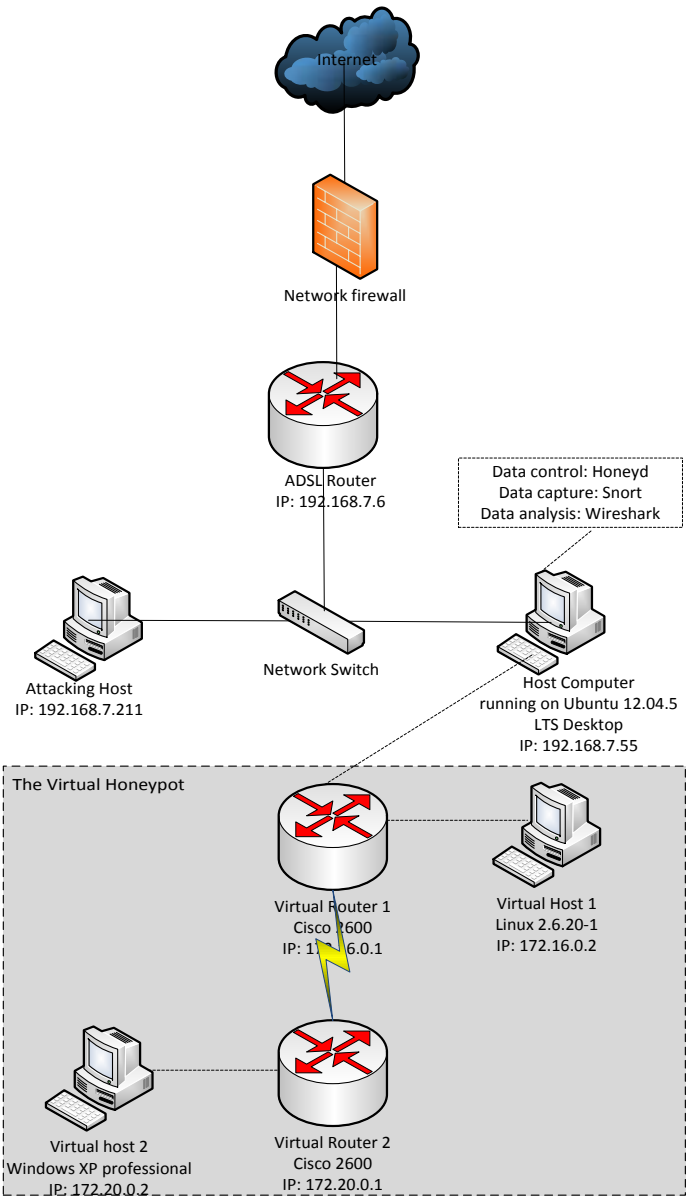

FIGURE 1. IMPLEMENTED SYSTEM ARCHITECTURAL DESIGN

3.2 Configuring the Honeyd

When configuring the Honeyd software to set up the virtual honeypot, it must be ensured that IP forwarding is disabled on the host computer that houses the Honeyd (Provos & Holz, 2008).If IP forwarding is enabled, then IP packets which the Honeyd receives for the virtual honeypots are forwarded to another computer in the 192.168.7.0 network where the host computer is located. In order to disable IP forwarding, the command below was issued on the host computer:

echo 0 > /proc/sys/net/ipv4/ip_forward

Before running Honeyd, it was ensured that the host computer can answer to all ARP requests which are sent by the router for the IPs of the virtual honeypots. This is achieved using the farpd tool for spoofing the ARP requests (Provos, 2008). It listens on the host network interface, i.e. the 192.168.7.0 network interface and responds with the MAC address of the Honeyd for the received ARP requests on the corresponding IP addresses. The incoming packets can be received through the Honeyd network interface with the help of the farpd. It allows for easy monitoring and capturing traffics which are sent to the virtual honeypots. This is achieved by running the following command on the host computer:

farpd <IP address of virtual honeypot]> -i eth0

where eth0 is the physical network interface of the host computer. shell), TCP port 20 (FTP), TCP port 88 (Kerberos authentication system) and UDP port 161 (SNMP). These ports are set to open for the attacker to establish connections to the virtual honeypot network only and it's not made to run any scripts or log any activities as these activities are implemented with the snort IDS system. The drop action is used to drop the entire packet to the port by default. Honeyd runs as a background process and as a user nobody which provides the security embedded within the Honeyd framework. In order to run the Honeyd configuration from the honeyd.conf file, the following command was issued on the host computer

Some part of the main commands used in the Honeyd configuration file to set up the virtual honeypot network is shown in table 1:

TABLE I. HONEYD CONFIGURATION COMMAND

```
####### Honeyd configuration file #############

create linux

set linux personality "linux 2.6.20-1 (Fedora Core S)"

set linux uptime 5184000 # sixty days

set 172.16.0.2 ethernet "3f:12:4e:14:d0:32"

set linux default tcp action block

set linux ethernet "Dell"

add linux tcp port 23 open

add linux tcp port 22 open

add linux tcp port 20 open

add linux tcp port 88 open

add linux udp port 161 0pen
```

The create command creates a template whose personality is 'linux' and it binds the honeypot's IP address to the personality. The set and add commands is used to change the configuration of the personality. The set command helps to assign the personality "linux 2,6.20-1 (Fedora Core S)" from the Nmap fingerprinting file. The uptime of the host shows how long the system has been running. The uptime was spoofed to be equal to 60 days i.e. 5184000 seconds to give enough room from the time of writing the configuration of the virtual honeypot to the time when the attack will be simulated. The add command opens the ports on the virtual honeypot, and specifies which services should run on each port. For the attacker to feel that it is attacking a real system on a real network, the open action is used to open most of the well-known ports such as the TCP port 23 (telnet), TCP port 22 (secure:

honeyd -d -i eth0 172.16.0.0/16 172.20.0.0/16 -f/etc/honeypot/honeyd.conf

At this point, Honeyd start listening on eth0 interface and answering to the packets for the network address 172.16.0.0/16 and 172.20.0.0/16 respectively of the configured virtual honeypots.

Ping, Nmap, telnet and traceroute tools was used to test that the Honeyd installation is working as configured and also to see if it is correctly receiving network traffic.

3.3 **Configuring the Snort IDS**

According to (Roesch, et al., 2015), Mostly all network cards have features named "Large Receive Offload" (lro) and "Generic Receive Offload" (gro). With these features enabled, the network card performs packet reassembly before they become processed by the kernel. Therefore, it is recommended to turn off both the LRO and GRO because Snort will truncate packets larger than the default snaplen of 1518 bytes. To disable LRO and GRO the following command was run on the host computer:

```
sudo apt-get install -y ethool
sudo ethool -K eth0 gro off
sudo ethool -K eth0 lro off
```

After snort was installed, some files and directories which are required by snort were created and permissions were set on the files. Snort keeps all configurations and rule files in etc/snort, and all alerts generated by Snort will be logged to /var/log/snort. This is achieved running the following commands on the host network

```
sudo groupadd snort
sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort
sudo mkdir /etc/snort
sudo mkdir /etc/snort/rules
sudo mkdir /etc/snort/preproc_rules
sudo touch /etc/snort/rules/white_list.rules /etc/snort/rules/black_list.rules
/etc/snort/rules/local.rule
sudo mkdir  /var/log/snort
sudo mkdir /usr/local/lib/snort_dynamicrule
sudo chmod -R 5775 /etc/snort
sudo chmod -R 5775 /var/log/snort
sudo chmod -R 5775 /usr/local/lib/snort_dyamicrules
sudo chown -R snort:snort /etc/snort
sudo chown -R snort:snort /var/log/snort
sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules
```

In order to write the configuration for snort to capture the ongoing communications with the different protocols configured on the Honeyd, the Snort configurations file at *etc/snort/snort.conf*. When snort is run with this file as an argument, it tells snort to run in NIDS mode.

Before Snort is ran, some edits were made to the default configuration file by commenting out of individual rule files that are referenced in the snort configuration file. The following line of command was used to out all the ruleset in the snort.conf file

```
sudo sed -i 's/include \$RULE_PATH/#include \$RULE\_PATH/ ' /etc/snort/snort.conf
```

In order to change the configuration file, Gedit text editor was installed and the following command was used to edit the snort.conf file

```
sudo gedit /etc/snort/snort.conf
```

Because the attack sequence to be alerted by the Snort software were to be simulated, the Snort rules to capture the costumed attack signatures as written in the local.rule configuration file. The local.rule file was enabled by uncommenting the *#include $RULE_PATH/local.rule.* Once the configuration file is ready, Snort will verify that the file is valid and all the necessary files that it references were correct.

Currently, Snort does not have any loaded rules i.e., the rule files referenced in snort.conf is empty. The Snort rule was written into the *etc//snort/rules/local.rule.* By uncommenting the *#include $RULE_PATH/local.rule* on the Snort configuration file, Snort was instructed that the local.rule files should be loaded. When Snort loads the file on start up, it will see the rule that was created and the rule will be implemented on all traffic incoming and outgoing on the eth0 interface.

To alert every ICMP packets that is moving through the eth0 interface, the following command was written into the *etc/snort/rules/local.rule* file

```
alert ICMP any any -> $HOME_NET any (msg:"ICMP alert" ; sid :10000001; rev:001;)
```

The diagram in Figure 2 shows the captured message on the Snort console.

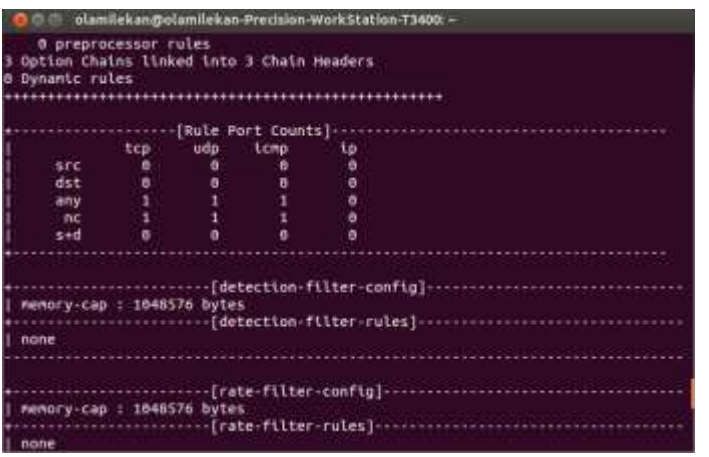

FIGURE 3. SHOWING THE RULE PORT COUNT

As seen from the Figure 2 above, the Snort IDS have could detect rules for any ICMP, UDP and TCP packets that is destined for the host computer through the eth0 interface. Snort was then started in the NIDS mode, and was told to

output any alert directly to the console. Snort was run from the command line : using the following flags

-A console	The 'console' option prints fast mode alert to stdout
-q	Quiet mode. Don't show banner and status report
-u snort	Run Snort as the following user after startup
-g snort	Run Snort as the following group after startup
-c /etc/snort/snort.conf	The path to the snort.conf file
-i eth0	The interface to listen to

The command issued according to the flag listed above is shown thus:

```
sudo /usr/local/bin/snort -A console -q -u snort
-g snort -c /etc.snort/snort.conf -i eth0
```

3.4 Configuring the Wireshark

The host system is configured with a DEB-based distribution, i.e. the Ubuntu 12.04.4 LTS operating system, Wireshark was installed from system repositories through the terminal window and the following commands were used:

```
Sudo apt-get install wireshark
```

4. Validation of Result

In this section, some validation test was carried out to verify the workability of the implemented system by carrying out different attack simulation on the system setup.

Hping3 (Sanfilippo, 2010) was used to launch simulated attack on the virtual honeypot setup to test the functionality of the system. The simulation does not actually project a hacking scenario, it proves to be effective in checking how the virtual honeypot works, how the Snort IDS logs the simulated attack sequence and how the data is captured using the Wireshark network protocol analyzer. The hping3 was installed in the attacking host shown in the diagram in Figure 1. Attacks to simulate the launching TCP, UDP and ICMP packets are being directed to the honeypot setup. The command that is used to carry out the attack sequence is the hping3 command. It requires administrative privileges to run it from the attacking host machine. The attacking host machine is presumed to be located on the production network i.e. it simulates that an attacker has hacked into the production network and has gained access to the network facilities with the rights to communicate with every computer on the production network including the virtual honeypots setup with the aim of bringing down the network and causing downtime.

A general hping3 command that can be used to send attacking packets to a host is shown below

```
#hping3 <victim IP> -V –c 1000000 –d 512 –S –w 32 –flood –rand-source
```

Also, to spoof the source IP address, the –a command option can be used. When the spoofing option is used, the source IP of the attacker is concealed, albeit the honeypot system still detects the attack. The command option used by hping3 is shown below.

V	Verbose-mode
c	Packet-count
d	Data-size
S	SYN flag
w	Window-size

4.1 Scenario 1: Use of TCP SYN Flag to Flood the Host Machine

The command used to create a TCP SYN flag flood on the attacker's machine is shown below

```
#hping3 <Victim's IP> -V -c 10000 –d 512 –S –w 32 --flood
```

Immediately the command is run from the attacking host, connection is setup with the honeypot and data is being received through the TCP protocol. To receive TCP connection with the host computer, it uses the SYN flag and an acknowledgement is received for the connection. As soon as a connection is established, the command allows TCP packets to flood the host (victim's) computer. These activities are captured and logged against the Snort IDS rule and the result

is output to its console. The Wireshark application is also started to listen on the eth0 interface where the virtual honeypot (Honeyd) and the Snort IDS is also configured. The figure 3 below shows the data that was logged and captured

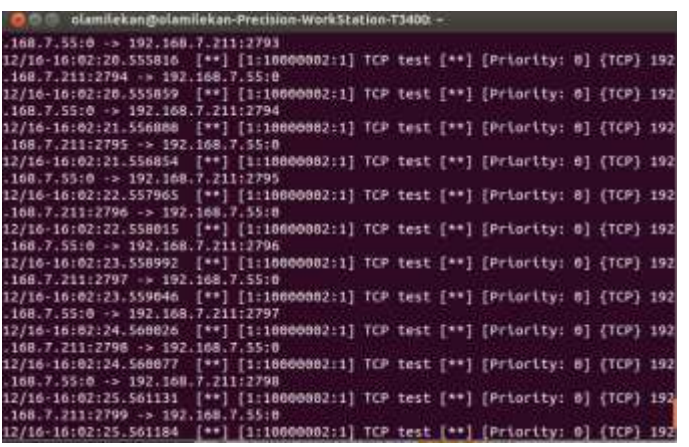

FIGURE 3. SNORT ALERT OF THE TCP FLOOD

Data from Figure 3 show that TCP packets are being sent from a source IP address of 192.168.7.211 which shows that the attacker is on the same subnet as the honeypot system. Once the command to run the Snort IDS is started, the TCP packed flood begins to be logged on the console. The first line from the figure shows how both host negotiates connections with every packet sent and every alert logged. An acknowledgment is also received at the reverse end of the communication. The host system established the connection using a dynamically assigned port number which it held for the length of the communication, while the assigned outgoing TCP port of the attacking host increases with a value of 1 for the next establishment of connection. The log also shows the output message configured on the local.rule file of the Snort IDS, showing both the sequence number and the priority level of the rule.

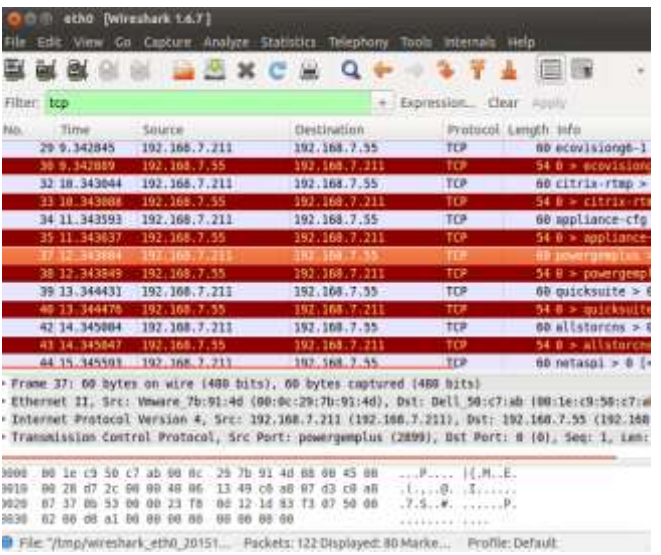

FIGURE 4. WIRESHARK CAPTURED TCP DATA

The Wireshark provides more insight to the TCP attack flood, when it is filtered to express TCP transactions only. The details from the frame number 37 selected above depicts a sent TCP frame from the attacker's machine. It shows the attacking host MAC address and the type of computer from which the attack is propagated (in this case a VMware machine). This data can help to track the location of the attacker and to prosecute them. It also shows the aggregated amount of flow, source byte, source packet, and destination flow and destination packets. The large amount of TCP flow confirms the flooded data from source to destination.

4.2 Scenario 2: Use of UDP Packets to Flood the Host Machine

The command used to launch the UDP flood attack on the honeypot system in this scenario is shown below:

```
#hping3 <Victim's IP> -V -c 10000 –d 512 –S –w 32 -2 --flood
```

The difference from the command used to flood the TCP packets is the -2 command. It is the hping3 command hat is used to flood UDP packets. The default command without the -2 will only launch TCP packets. Since UDP does not require a connection establishment like the TCP, the attacking host starts sending packets immediately the command is run. The Snort IDS alert is shown in Figure 5.

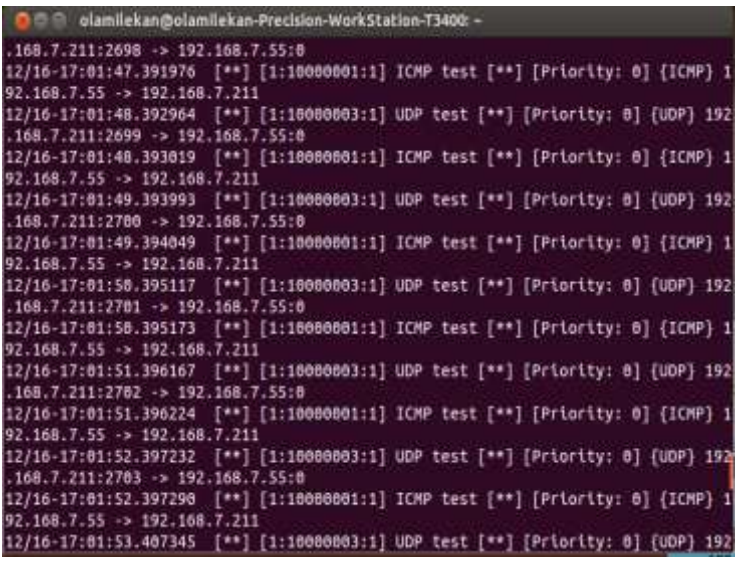

FIGURE 5. SNORT CAPTURE OF UDP FLOOD PACKETS

The Snort IDS logs an ICMP packet every time a UDP packet is sent to the honeypot system. The hping3 tool uses the ICMP to generate a form of connection with the host before flooding it with the UDP packet. The destination port is 0 but all the unassigned port numbers between 0-65535 was used by the attacking host to flood the UDP packets.

The Wireshark capture also depicts both the ICMP and UDP packets and the highlighted UDP packet also shows the time the packet is sent in seconds, the source and destination address of the UDP packet. The Figure 6 below shows the Wireshark capture

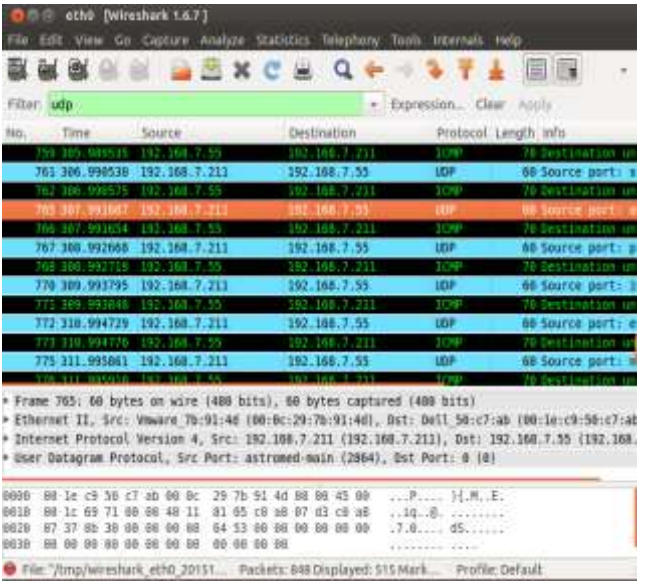

FIGURE 6. WIRESHARK UDP FLOOD CAPTURE

4.3 Scenario 3: Use of ICMP Packets to Flood the Host Machine

The command used to launch the ICMP flood attack on the honeypot system in this scenario is shown below:

```
#hping3 <Victim's IP> -V -c 10000 –d 512 –S –w 32 -1 --flood
```

The -1 command of the hping3 was used to generate the ICMP packet in this scenario. The Snort IDS capture is shown Figure 7.

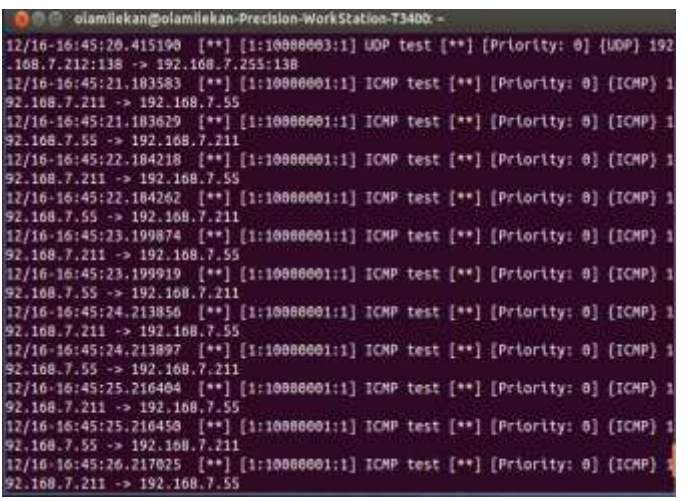

FIGURE 7. SNORT CAPTURE OF THE ICMP FLOOD

As seen from figure 7, the rule captured the ICMP packets coming from the attacking host computer and it was logged on the console of the Snort IDS. The source, destination and port numbers are shown as well.

5. Conclusion

In this paper, a virtual honeypot setup that combines Intrusion Detection System has been presented. It can capture all types data proposed to be used to attack the network which includes TCP, UDP and ICMP, and it also gives a lot of information about the attacking protocols via the Wireshark network analyzing tool. Alerts from the Snort IDS console and captures from Wireshark reveals the protocols the attacker is using.

Honeypots whether physical or virtual are meant to emulate real production networks at a level of operation, mostly deploying the protocols that attackers find interesting to obliterate. It is not of full guarantee that a network would be attacked or spoofed and most of the security defense system might just end up being redundant. This option will be sure to provide a cheaper solution for the decoy system.

References

Roesch, M., 2015. *Snort.* [Online] Available at: https://www.snort.org

Amitabh, M., Ketan, N. & Animesh, P., 2004. Intrusion Detection in Wireless Ad Hoc Ntwork. *IEEE wirless communications*, Issue 04, pp. 48-60.

Annamma , A., Runuka, P. B. & Abhas, A., 2011. Design and Efficient Deployment of Honeypot and Dynamic Rule Based Live Network Intrusion Collaborative System. *International Journal of Network Security & its Application*, III(2), pp. 52-65.

Anuar, N. B., Zakaria, O. & Yao, C. W., 2006. Honeypot Through Web (Honeyd@WEB): The Emeging of Security Application Integration. *Informing Science and Information Technology*, III(1), pp. 47-56.

Ghorbani, A. A., Lu, W. & Tavallaee, M., 2010. *Network Intrusion Detection and Prevention.* 1st ed. Boston: Springer Verlag.

Kaur, G. & Saini, J. S., 2013. Implementation of High Interaction Honeypot to Analyse The Network Traffic and Prevention of Attacks on Protocol/Port Basis. *International Journal of Computer Application*, LXII(16), pp. 22-29.

Provos, N., 2008. *Development of the Honeyd Virtual Honeypot.* [Online] Available at: http://www.honeyd.org/

Provos, N. & Holz, T., 2008. *Virtual Honeypots: From Botnet Tracking to Intrusion Detection.* 1st ed. Boston: Pearson Education, Inc..

Richardson, R., 2010. *2010/2011 CSI/FBI Computer Crime and Security Survey.* [Online] Available at: http://gatton.uky.edu/FACULTY/PAYNE/ACC324/CSISurvey2010.pdf [Accessed 12 June 2015].

Roesch, M., Green, C. & Caswell, B., 2015. *The Snort project: Snort 2.9.7.3.* [Online] Available at: https://s3. Amazon ws.com/snort-org-

site/production/document_files/files/000/000/086/original/snort_manual.pdf

Sabah, S. & Vandana, D., 2013. Roaming Honeypots Along With IDS in Mobile Ad-Hoc Networks. *International Journal of Computer Application*, LXIX(23), pp. 15-21.

Sanfilippo, S., 2010. *Hping Manpage.* [Online] Available at: http://www.hping.org [Accessed 15 February 2017].

Vollmer, T. & Manic, M., 2014. Cyber-Physical System Security with Deceptive Virtual Host for Industrial Control Networks. *IEEE Transanctions on Industrial Informatics*, X(2), pp. 1337-1347.

Wang, J. & Zeng, J., 2011. Construction of large-scale Honeynet Based on Honeyd. *Procedia Engineering, 2011, Vol.15, pp.3260-3264*, XV(1), pp. 3260-3264.

Weizhe , Z., Hui , H. & Tai-hoon , K., 2013. Xen-based Virtual Honeypot System for Smart Device. *Springer Science and Business Media*, III(2), pp. 1-18.

Zhou, Z., Chen Zhongwen, Z., Zhou Tiecheng, Z. & Guan Xiaohui, Z., 2010,. The study on Network Intrusion Detection System of Snort. *International Conference on Networking and Digital Society*, II(1), pp. 194-196.

An Open Access Journal Available Online

Survey of Video Encryption Algorithms

Babatunde A.N.[1], **Jimoh, R.G.**[2], **Abikoye O.C.**[3] **& Isiaka B. Y.**[4]

Department of Computer Science,
College of Information and Communication Technology,
Kwara State University, Malete, Nigeria.
[1]drealak@gmail.com
Department of Computer Science,
Faculty of Communication and Information Sciences,
University of Ilorin, Ilorin
[2]jimoh_rasheed@yahoo.com
Department of Computer Science,
Faculty of Communication and Information Sciences,
University of Ilorin, Ilorin
[3] Kemi_adeoye@yahoo.com
Department of Computer Science,
College of Information and Communication Technology,
Kwara State University, Malete, Nigeria.
[4]yabolaji4@gmail.com

Abstract: Research on security of digital video transmission and storage has been gaining attention from researchers in recent times because of its usage in various applications and transmission of sensitive information through the internet. This is as a result of the swift development in efficient video compression techniques and internet technologies. Encryption which is the widely used technique in securing video communication and storage secures video data in compressed formats. This paper presents a survey of some existing video encryption techniques with an explanation on the concept of video compression. The review which also explored the performance metrics used in the evaluation and comparison of the performance of video encryption algorithms is being believed to give readers a quick summary of some of the available encryption techniques.

Keywords: Encryption, Video Security, Performance Metric, Compression, Decompression.

1. Introduction

The security of video data is becoming more important nowadays because of the rapid development in multimedia video compression and the latest development in internet technologies. These breakthroughs have enabled video data to be used as a medium through which sensitive information can be easily stored and transmitted. Hence, video data needs to be protected from unauthorized access during the cause of transmission and storage. Video encryption is the widely established and secured means of video content protection (Ajay et al., 2013; Yogita, 2013; Darshana & Parvinder, 2012; John & Manimurugan, 2012; Mayank et al., 2012; Jolly & Saxena, 2011).

Traditional ciphers which are based on the theory of number (algebra concept) which are the Advanced Encryption Standard (AES) and Data Encryption Standard (DES). These two methods are most straight forward approaches to total video security. Majority of these encoders are utilized for text and binary data that is due to huge volume of data are not fit for multimedia data. Developing a cryptosystem for video data using these traditional ciphers incur significant overhead and expensiveness in actual time video systems such as video conferencing and digital image surveillance (Zhaopin et al., 2012). Also, considering the fact that consecutive frames bear close resemblance, it is likely that a subtle amount of pixels might change from one frame to another. Hence, there is high data tautology in continuous image data which can be removed to ensure that the big size of the video data is reduced for easy transmission and storage. This is the reason traditional ciphers muff viewable information. (Zhaopin et al., 2012; Furht et al., 2005). Hence, there is need for efficient video compression techniques. Video compression is very important in the efficient transmission and storage of videos. This is because raw video data contains an immense amount of data and a high bit rate which increases the communication and storage requirements.

Video encryption algorithms generally works with videos in a compressed format because of its large volume nature to make its storage and transmission over bandwidth-limited networks feasible (Rajagopal & Shenbagavalli, 2013; Yogita, 2013; Mukut & Pradhan, 2011) An absolute solution for protecting video transmission cannot be provided by a single technology. (Eugene et al., 2001; Jolly & Saxena, 2011). Encryption of video data can however take place before, during or after compression.

2. Compression

2.1 Compression of Video

A video consist of series of discrete digital images exhibited at a fast succession with fixed magnitude. In videos, these images are called frames with each frame liable to resemble close frames. The magnitude at which frames are displayed is measured in (fps). A frame is digital image which is made up of pixel's rasters. A pixel is a small square with only one property called color. Hence, a frame with W pixels breadth and of H pixels height has a size of frame $W * H$ pixels.

Video compression is an engineering of video signals under constraint without losing its quality by utilizing data redundancy in between successive video frames. (Suganya & Mahesh, 2014). It is the process of encoding video data to contain fewer bits thereby allowing an effective data movement and storage. Compression is a reversible process whose inverse called decompression

reproduces the uncompressed video data (decoding). (Djordje, 2009).

In video compression, a small percentage of the original video bits is required by each frame hence assuming a compression algorithm shrinks an input multimedia data by a Compression Factor (CF):

Bit Rate (BR) = Bits per frame * frame rate where Bits per frame=$W * H * Color\ depth.$

$$= W * H * CD * FPS/CF$$

$$= W * H * \left(\frac{CD}{CF}\right) * FPS$$

Where $\frac{CD}{CF}$ is the average bit per pixel (BPP).

Thus,

$$BR = W * H * BPP * FPS \text{ and } VS = (BR * T) / CF$$

Bit rate is the amount of magnitude of information a digital video stream contains. Bit rate equates the quality of the video in uncompressed videos. Bit rate is an important feature during transmission. This is so because bit rate must be supported by a strong enough transmission link. Also, since the video size is proportional bit rate and duration.

The average Bits Per Pixel (BPP) is a measure of the efficiency of compression, a true color with no compression may have a BPP of 24 bits per pixel.

2.2 Types of Video Compression

There are two types of video compression techniques; Compression can be lossy or lossless.

Lossless compression: In this type of compression, compression doesn't relinquish any visual content or details carried by initial data. The original data is not distorted. Here, the degree of compression is limited. It permits a recovery of 100% original data recovery. This method is employed when loss of information causes a major damage. (Djordje, 2009). Examples includes the Huffman algorithm, Run length coding etc,

Lossy compression: In a lossy compression, a higher compression rate can be achieved by removing unnecessary information which are not obvious to the viewers and will not change the subjective quality of the decoded video signal. It is employed in data which contain lot of redundancies and insensitive to losses. In Lossy compression some information that cannot be recovered are destroyed, that is original data cannot be recovered in this technique. (Hosseini, 2012). However, the recovered information is useful in some ways. (Sashikala et al., 2013; Djordje, 2009).

2.3 Video Compression Format

A lot of video compression as well as codec algorithms such as the intel RTV/ indeo, IBM photo motion, moving Joint Photographic Experts Group (MJPEG), wavelets, H.261/H263, Moving Picture Experts Group (MPEG) have been reported in literature in the last three (3) decades but our current interest is on MPEG compression.

MPEG (Moving Picture Coding Experts Group) compression whose founding fathers are Leonardo Chairigline (Italian) and Hiroshi Yasuda (Japan) has a basic idea in transforming a stream of discrete samples into a bit stream of token such that it take a less space. A video stream is series of digital pictures.

MPEG makes use of the temporal relationship between successive frames for compression of video streams. (Hosseini, 2012). The basic principle behind MPEG video compression is image to image prediction.

MPEG and some video compression algorithms utilized in standards usually contain the following: reduction in resolution, motion estimation, Discrete Cosine Transformation (DCT), entropy coding and quantization. One very important step is the motion estimation.

The motion compensation is the procedure through which the positions between diverse types of frames are obtained. In motion compensation, MPEG video can be defined as series of frames. Frames in this series are coded using three (3) different categories of frames. We have I-frame which is also called the intra-frame, the predicted frame referred to as P-frame and the bi-directional frame referred to as B-frame. The P and B- frames are referred to as inter-coded frames.

The self-contained frames which is also known as I-frame are called the key frames. They have no correspondence to other frames. These are employed as access points in MPEG streams and are coded using a discrete cosine-based approach related to JPEG format. To decode any frame, one needs to search and find the closest previous I-frame. This is done to allow reverse playback, skip ahead or error recovery. (Hosseini, 2012; Sayood, 2003). They produce the lowest compression ratio within the three frames. (Hosseini, 2012; Raymond and furht, 1997; Djordje, 2009).

P-frames which is known as the predicted frames are frames of previous I-frame or P-frame. These are coded using forward predictive coding. The purpose of coding P-frames is to find matching images that are of related forms in the preceding corresponding frame then code just the dissimilarity in the P-frame and the matching being found. For individual main block in the frame, the encoder locates a corresponding block in the former P-frame or I-frame which is considered the best match for it. The corresponding block can potentially be anywhere in the image. Once exact frame is identified, the pixels of the corresponding block are deducted from the referencing pixels in the main block. This give a result of residual value that is near zero. This residual is coded using a similar approach to JPEG algorithm. There is need for a coder to send the motion vector which is achieved using Huffman compression algorithm. If there is no match located, then the block would be coded the same as an I-frame. (Hosseini, 2012). Less space is required in this frame as compared with the I-frame as only the differences are stored. Also, the compression ratio here is appreciably higher than that of I-frames. (Raymond and furht, 1997; Djordje, 2009).

B-frames which are referred to the bi-directional frames are coded using two different directional corresponding frames (forward and backward frame) which can be I-frame or P- frame. In this type of frame, a reusable data is looked for in both directions. This approach is like P-frames but instead of just looking for the former I or P-frame for a match the next I or P- frame is looked for in the method. If a match is identified for the two directions, the average of the two (2) reference frames

is used. If only one good match is found, then the one found will be used as the reference. In cases like this the coder must pass information specifying the corresponding that was employed. (Hosseini, 2012; Lelewer and Hirscherg, 1987). B-frame provides the highest amount of compression. (Raymond and furht, 1997; Djordje, 2009).

The particular frame used in a video determines the compression and quality ratio of the video compression. I-frames increases value and dimensions while B-frames reduces better but gives a poor value. The length that exists between 2 I-frames measures the quality of an MPEG-video. Motion vector is the relationship between 2 frames in terms of motion. The motion vector and the arithmetic difference depend on effectiveness of the implemented motion compensation algorithm. Motion compensation operation is computationally intensive which usually not suitable for real-time applications. (Djordje, 2009). It is a process that involves frame segmentation, search threshold, block matching, prediction error coding and vector coding.

Some common examples of MPEG algorithms include MPEG-1, MPEG-2 and MPEG-4.

Moving JPEG (IS92a) uses the Joint Photographic Experts Group (JPEG) to provide compression for each frame of the video and hence providing a randomized access to individual frames. Compression ratio in this standard is very low as the algorithm considers not the advantage of similarities between adjacent frames. (Raymond and Furht, 1997).

MPEG 1 (IS92b) on the other hand supports the compression of image resolutions of about $352 * 288$ pixels at 30fps into a data stream of 1.5mb/s. It allows fast forward and backward search with synchronization of audio and video.

MPEG-2 (IS93b) is a quality supporting reduction of digital image resolution of just about $704 * 576\ pixels\ at\ 30fps$ and $HDTV\ of\ 1920 * 1152\ at\ 60fps$. It compresses approximately at three (3) times that of moving JPEG. It is compatible with MPEG 1 but allows a better quality with a slightly higher bandwidth of between 2 and 20 Mbits/sec. The development of MPEG-2 had extra emphasis on scalability with the ability of playing different resolutions and frame rates of a video. MPEG-2 was designed because of the inability of MPEG-1 to be used in audio coding and video quality for television broadcasting systems and also its inability to efficiently encode interlaced fields. MPEG-2 aids the recovery from errors in transmission as some error recovery mechanisms were used with the encoder. (Raymond and Furht, 1997).

MPEG-4 was released in late 1998 with a main development over MPEG 2. This was developed for use in environments that are interactive such as multimedia application and video communication (Djordje, 2009). It has a bit rate of between 10kbits/sec to 1Mbits/sec. MPEG-4 has the ability of regrouping the content of a frame into objects which individual can access through the MPEG-4 syntactic description language (MSDL). MPEG-4 can reduce the bit

rate independently for certain applications and they are adaptive to specific areas of video application. Its other characteristics include robustness in error-prone environments, improved coding efficiency, improved temporal random access etc. It supports both MPEG-1 and MPEG-2 functionalities although many of the tools in MPEG-4 need enormous computational ability (for encoding and decoding) this makes then not practically applicable for most normal and non-experts or real-time systems.

The usage of MPEG has touched so many real-life applications like cable television, broadcast satellite that is not interrupted, real-time encoding, computer network etc.

2.4 Data Redundancies

Video compression is feasible because video data contains a lot of redundancies. However, it must be noted that there is always a trader-off between quality and data size when compression methods are employed. The higher the ratio of compression, the smaller the size of the video and the lower the video quality.

2.4.1 Types of Data Redundancies

There are basically two (2) categories of redundancy in a video data; the spatial redundancy and temporal redundancy. Spatial redundancy: In a frame of a video data, nearby pixels are often correlated (related) with each other, this correlation is called intra-frame correlation, that is, Spatial redundancy is divided into two types: the statistical and redundancy in subjective type. Redundancy in statistical type simply mentions that the neighbouring values of pixel in digital image are frequently much correlated. Entropy coding such as Huffman coding can be applied to remove this type of redundancy. Redundancy in subjective type on the other hand mentions that human visual system is invariant to particular visual information parts. Hence, these parts may be taken away without resulting to serious subjective standard degradation.

Temporal redundancy: (inter-frame correlation) means adjacent (neighboring) frames are highly correlated, that is, within a sequence of video, successive frames are usually the same. The movement in the scene is usually due to differences between successive frames. Similarity in two successive frames in a sequence, result to a condition in which many of the blocks in the difference frame have no information and this indicates no further need of any transmission.

In other words, to have a well compressed video, the spatial and temporal redundancy must be efficiently reduced. There are basically three (3) factors to be considered during the compression process: the image size, the color depth and the frame size.

Image Size: complete screen resolution is normally 640 x 480 pixels or 800 x 600 pixels for a 14 inch monitor. Just like in frame rate, compressing the image size can greatly reduce file volume. When reducing an image dimensions, a 4:3 aspect ratio should be used. Aspect ratio of a digital image represents the proportional relationship between an image width and its length. It is quite possible to play back a 320 x 240 image sized video at double-size to have a complete-screen movie with

practically good results. A small video size would normally run at 192 x 144 pixels.

Color Depth: Normal digital video has 24-bit colour (millions of colours). Cutting down the colour range to 16 bit (thousands of colours) will reduce file size by one third. Some codecs permit 8-bit color (256 colors) which only might work for animations.

Frame Rate: A raw video runs 30 frames per second. Although, the illusion of motion can still be obtained with speeds as slow as 10 frames per second when there are no speedy moving objects. Cutting the speed to 15 frames per second or less can reduce the size of a file in half (or less than half) without sacrificing quality when there is only a moderate amount of motion. Evaluations should be conducted on the video file to determine which colour depth is important because reducing colour depth can really affect the image.

3. Encryption

3.1 Introduction

Data encryption is an appropriate method of protecting video data from unauthorized access. Various traditional ciphers have been proposed but are more suitable for text and binary data. As video data comprises of enormous volume, it is herculean to use these encoders in video protection.

3.2 Classification of Encryption

Typically, Video encoding techniques can be grouped into four basic types; completely layered technique, permutation based technique, selective encryption technique and perceptual technique. (Ajay et al., 2013; Yogita, 2013; Zhaopin et al., 2012; Jolly and Saxena, 2011).

Completely Layered Encryption: In a completely layered encryption, a cryptosystem is used in the encryption process to encrypt the whole video data after being compressed without considering any region of interest. Encryption is done on the video data frame by frame without considering the objects in video or any other important information. They produce the highest security and they have higher computational Intricacy than the other groups more adequate for securing video storage (Zhaopin et al., 2012; Wong and Bishop, 2005). Due to their high computational demand they are not applicable to real-time video applications (Jolly & Saxena, 2011). Examples of this group can be found in the techniques developed by some researchers (Li et al., 2002; Ganesan et al., 2008).

Selectively Encryption: In a bid to reduce the computational complexity inherited as a result of encrypting the whole video data, algorithms that selectively encrypts a particular video sizes (bytes) within the video frames were designed. These methods selectively encrypts only sensitive or important bytes in the video frames. Although these methods lessen complexity in computation through selection of simply the least set of data encode but the protection and pace level is dependent on how many protected parameters. (Jolly and Saxena, 2011). The works proposed by Spanos and Maples, 1995; Meyer and Gadegast, 1995; Shi and Bhargava, 1998; Wu and Kuo, 2001 etc are examples of algorithms in this group.

Perceptual Encryption: the perceptual encoding needs the audio/video quality

of the data be partially devalued such that the encoded data are still partly perceptible after encoding and the audio/ video quality of the data is continuously controlled. Perceptual encryption algorithms are unsuitable for applications which require high security. They are suitable only for entertainment applications like pay per view. (Jolly and Saxena, 2011). The works proposed by Pazarci-Dipcin, 2002; Lian, Wang, Sung and Wang, 2004 etc are examples of algorithms proposed in this category.

Permutation Encryption: The permutation based encryption uses diverse permutation technique s to scramble or protect video contents. The entire video does not necessarily need to be scrambled as a particular set of bytes might be scrambled and a permutation list is applied to serve as a secret key. Permutation based algorithms are generally fast but provides an insufficient level of security. (Jolly and Saxena, 2011). Pure permutation, Zig-zag permutation (Tang, 1996), Huffman code word (1998), correlation preserving (2006) etc are examples of algorithms in this category.

As explained above out of the four (4) classifications, it has been proved and shown that the completely layered video encryption produces the highest level of video security but it is computationally expensive because of its slow nature in processing the very large volume of video data and has in return limited its use in video encryption. (Darshana and Parvinder, 2012; Jolly and Saxena, 2011; Abomhara et al., 2010; Puech et al., 2012).

3.3 Performance Parameter

Many encryption of video techniques have been designed. Irrespective of the classification of any designed encryption technique falls into, the following metrics are being used to evaluate and compare their performance. (Ajay et al., 2013; Darshana and Parvinder, 2012; Zhaopin et al., 2012; Jolly and Saxena, 2011).

Security: In most video employment, several levels of protection for capability of complex processing although most cryptographic applications are completely or partly ascendible meaning different security levels are chosen. To achieve scalability, sizes in key or iterations of different values are allowed. A very high security level is attained with number of iterations or larger key.

The encryption technique security is commonly tested by continuous analysis of key space, experiments, analysis of key sensitivity and invulnerability to attacks.

Continuous experimental result is accomplished through class of comparison that exist in the encrypted data and first (original) multimedia data.

Key space analysis is a procedure that involves the application of number of keys analysis encryption process e.g. a bit of 20 key would give 2^{20} key space.

Sensitivity of key for example in a disordered cipher mentions the original levels of sensitivity and control parameters sensitivity of chaotic map.

A method of encryption should be not affected with cryptanalytic attacks such as identified (known) plaintext attack, chosen plaintext attack, brute force attack etc. (Ajay et al., 2013; Darshana

and Parvinder, 2012; Zhaopin et al., 2012; Jolly and Saxena, 2011).

Transmission Error Tolerance: The real time passage of multimedia data frequently happens in noisy environments, this is right in the case of wireless networks where the delivered data is liable to bit errors. It is highly desirable that technique of encryption be unaffected and invariant to errors in transmission. The robustness of a video transmitted over a network can be tested by correctly decrypting data encrypted not considering whether some bytes or a frame are degraded or lost during the process of transmission. A fault tolerant is a scheme of encryption that does not affect format of file and its small modification in a pixel does not spread to others. This can also be done by analyzing the relationship in the frames decrypted quality and bit-error number that occurred in the frames that are encrypted (Ajay et al., 2013; Darshana and Parvinder, 2012; Zhaopin et al., 2012; Jolly and Saxena, 2011).

Encryption Ratio: Encryption ratio can be defined as proportion between encrypted video size and the complete data size. Encryption ratio has to be minimized as much as possible to reduce computational complexity. (Ajay et al., 2013; Darshana and Parvinder, 2012; Zhaopin et al., 2012; Jolly and Saxena, 2011).

Compression Efficiency: Compression is performed on video data because of their large size to minimize storage space and bandwidth usage. The encryption method can be achieved earlier, in the course or after compression. Whichever time process of encryption is carried out, the encrypted video size must be made as small as possible. (Ajay et al., 2013; Darshana and Parvinder, 2012; Zhaopin et al., 2012; Jolly and Saxena, 2011).

Degradation: Video distortion can be measured by visual degradation. Visual degradation may be low or high. For example, video sensitive applications such as video conferencing in business gatherings require a great visual degradation while for an entertainment application a low degradation may be needed. (Ajay et al., 2013; Darshana and Parvinder, 2012; Zhaopin et al., 2012; Jolly and Saxena, 2011).

Computational Efficiency: This is defined by its space and complexity in time of encryption algorithm. Complexity in space of an encoding algorithm is the memory required by the program to run while complexity in time is encryption or decryption time. There is however need for a small encryption size and decryption technique with also fast algorithms to meet real-time requirements for applications in video. (Ajay et al., 2013; Darshana and Parvinder, 2012; Zhaopin et al., 2012; Jolly and Saxena, 2011).

Lossless Visual Quality: This is an extremely desirable feature for applications in entertainment. Algorithms in encryption should be able to give the same visual quality as initial video when decrypted properly. (Ajay et al., 2013; Darshana and Parvinder, 2012; Zhaopin et al., 2012; Jolly and Saxena, 2011).

Format Compliance: As a result of the enormity of data in multimedia and irrelevant data, the encoding of data are usually performed before transmission which produces data streams with some

format information. This format information will be used by the decrypter to regain a successful multimedia data. It is wished that the multimedia format is kept by the encoding algorithm, that is, the bit stream encrypted should be conformable with the compressor. (Ajay et al., 2013; Darshana and Parvinder, 2012; Zhaopin et al., 2012; Jolly and Saxena, 2011).

3.4 Video Encryption Algorithm

This section reviews some encryption techniques that has being in literature in the last two (2) decades.

Ajay et al., 2013 proposed an encryption algorithm where a video cutter is used to separate the video into frames. These video frames are in video format as they contain audio data. A shuffling block shuffles these video frames which are then moved on to frame stitching block. A new video is formed by frames which are now in random position. In this technique, the audio stream cannot be decrypted unless one has the knowledge of the shuffling methodology. A random key generated by a function in java is used by the shuffling algorithm, this function is called shuffling key which is encrypted end to end with the video applying AES that is carried together with the video to the destination decryption block.

This algorithm will suffers from brute force attack. There is however need to increase the security strength of the algorithm. To achieve this, AES is used to encrypt the code words extracted from MVDs, DCs and ACs. Computational time is saved by extracting and encrypting only important or sensitive code or words. Code words are after encryption mixed-up with the blocks on every frame remaining the same but with a changed location. The video is however sent to the client who runs the algorithm in AES over the code words to decrypt and also to get a standard video. The decryption block also decodes the random key and apply it to restructure frames to its initial location. The proposed algorithm has a very good computational speed and a high level of security.

Mayank et al., 2012 proposed an encryption scheme which is based on the encryption of I-video frames by using an effective and generalized scheme based on computation in matrix. This system applies the concept of video frame and XOR operation. They made use of knowledge of matrix computation for generating the encrypted I-frame. All video frames were collected then were taken one after the other and a key frame selected as the key image for the encoding and decoding process. A secured channel is used to send key image. The remaining frames were encrypted by their designed algorithm and after the encryption algorithm has been applied on all frames, they were combined to form an encrypted video. This scheme is efficient and secured against a cryptographic but it can only be applied to a certain class of video sequence and video codes. (Yogita, 2013).

Saranya & Varalakshimi, 2011 proposed a selective video encryption with the purpose of selecting an adequate data in advance the compression for encryption which in return gives a greater efficiency at a reduced cost. They proposed a distinct scheme with RC4 stream ciphers which is used to generate

a pseudorandom stream of bits in which the encryption is combined with the plaintext using bit-wise exclusive-or with the decryption executed in the same manner. (Rajagopal & Shenbagavalli, 2013)

Shaima and Khalid, 2011 came up with an in-compression algorithm for encryption applying Optimized Multiple Huffman Table (OMFT). This technique encodes and encrypts video sequence. It encodes video sequence frame or encrypts the original frame and then reduce and encrypt the motion vector between successive frames. The OMHT encryption technique and the OMHT process takes two (2) parallel paths. No extra time is required to include encryption to the compressed bit stream as both in traditional and selective encryption technique. A statistical model based compression is used to generate different tables from a training set of videos. An increased compression efficiency and security is attained. (Rajagopal & Shenbagavalli, 2013)

Yan and Main, 2009 designed a video encryption system by applying scrambling to the Discrete Cosine Transform (DCT) coefficient in a 16 x 16 macro-block. They used a complete scrambling algorithm to disorder DCT coefficients in the macro-block, a subsection scrambling algorithm to divide the DCT coefficients and scrambles them in different segments according to security and compression ratio. In this video cryptosystem, the encrypted DCT coefficients scrambling algorithm only breaks the order of coefficients or macro-blocks and doesn't encrypt video data hence it has a low security. Also, because the technique requires only scrambling and not encryption, DCT coefficients scrambling algorithm has high runtime. (Rajagopal and Shenbagavalli, 2013).

Yang and Sun, 2008 developed a chaos-based video encryption method in a DCT (Discrete Cosine Transform) domain. In this CVED, only I-frames are selected as encryption objects, a double coupling logistic map is used to scramble the DCT coefficients of I-frames and then encrypt the DCT coefficients of the scrambled I-frames by using another logistic map. The technique is applicable in real-time applications as only encrypting the coefficients of I-frames consumes little time. The study introduced Five (5) keys in the complete process and thus the key space is large enough to resist brute force attack. This technique is not secured enough as there are some B and P-frames which are unprotected that are encoded without referring to I-frames. (Zhaopin et al., 2012).

Ganesan et al., 2008 designed a public key encryption (PKVE) of videos based on chaotic maps. In this technique, if the number of frames are so many, the phrase scrambling method proposed by Nishchal et al., 2013 will be used which will be followed by the encryption of video using the chebyshev maps (Bergamo et al., 2005). The entire video frame can as well be encrypted using Arnold transform (Prasad, 2010). This technique is secured over known chosen-plaintext intrusion and with high key sensitivity. It is very effective in real time application for 64x64 and 128x128 pixel size videos. (Zhaopin et al., 2012).

Li et al., 2002 proposed a chaotic video encryption (CVES) for real time digital video based on multiple digital chaotic

systems. In this technique, each plain block is first XORed by a chaotic signal and then replaced by a pseudo-random S-box based on multiple chaotic maps. This encryption technique is invariant to intrusion and known chosen-plaintext attacks. It has a reduced computational complexity and therefore can be easily utilized for hardware and software. (Zhaopin et al. 2012).

Chiaraluce et al., 2002 described an encryption algorithm for H.263 videos where the cipher operations were seamlessly combined with the H.263 encoding method, that is, RLC and packaging. In this encryption technique, the significant bit in the DC coefficient of DCT, the AC coefficient of I-MB (Intra macro blocks), the sign bit of the AC coefficients of the P-MB (predicted macro-blocks) and the sign bit of the motion vectors are encrypted applying three (3) properly arranged different chaotic functions namely the Skew tent mop, saw-tooth likewise map and logistic map. It has a key space of 2^{512} which is greatly sufficient over brute-force attack. It modifies key every 30 frame and thus secure against known chosen plaintext attacks, it however increases the time of processing. (Zhaopin et al. 2012)

Wu and Kuo, 2001 proposed 2 selective algorithms in encryption for MPEG video called the Multiple Huffman Tables (MHT) and MSI (Multiple State Indices) encryption algorithms. The first algorithm was based on encryption during entropy coding. At the entropy coding stage, symbols in the video stream are transformed to binary sequences in accordance to predefined Huffman table to integrate encryption with entropy coding. The basic MHT encryption work as; at first 2^k Huffman tables created and numbered 0 to 2^k -1 then random vector P of n numbers produced where each number is a K bit number in the range 0 to 2^k -1. The basic building block of this algorithm is that it converts entropy coders into encryption ciphers. (Darshana and Parvinder, 2012; Jolly and Saxena, 2011; Eisenbarth, 2007).

Not well satisfied with their work, they proposed an enhanced version of the MHT in 2005. A directional hash function was used to initiate a key hopper by first assigning some seed value S which is used and then produce the output values by applying a hash function on the seed value and further values generated from seed value like (S+1, S+2 etc). However, various cryptanalysis studies have shown that the basic and improved MHT techniques are at risk to selected plaintext and identified plaintext attacks. (Darshana and Parvinder, 2012; Jakimoski et al., 2008; Zhou et al., 2007). Also, encrypted videos using MHT scheme is completely incomprehensible and as such cannot be used for perceptual encryption. (Darshana and Parvinder, 2012).

Cheng and Li (2000) extended their limited encryption schemes to digital still images to continuous images (video). The scheme uses a quad tree compression method and wavelength compression algorithm based on zero trees for the video stream I-frame, motion compensation and residual error coding. The scheme works for video stream based on set partitioning in hierarchical trees image compression algorithm. The proposed encryption system encrypts the I-frames, the motion

vectors and residual error code of video stream. (Darshana and Parvinder, 2012).

Alattar et al (1999) proposed three (3) methods for selective video encryption of MPEG-I video sequence, based on DES cryptosystem. In the first cryptosystem, every n^{th} I-macro-block was encrypted. In the second method, headers of all the predicted macro-blocks and n^{th} macro-block data were encrypted. The third method encrypts n^{th} macro-block as well as the header of every n^{th} predicate macro-block. This scheme works during compression. (Darshana & Parvinder, 2012).

Shi and Bhawgava (1998) developed a video encryption algorithm (VEA) where an undisclosed key was employed to randomly alter the sign bits of the DCT coefficients of I-frame using the simple XOR operation. The maximum 64 bits of DCT sign values selected and XOR operation is accomplished with the key and due to the fact that only 64 bits of information is being encrypted for each frame the algorithm is very fast. This algorithm produces a very high-visual degradation because the DCT coefficients are being encrypted. The algorithm security is vulnerable to known plaintext attack and known cipher text attack. (Mukut & Pradhan, 2011).

They however improved their work by proposing an algorithm called the MPEG video encryption algorithm (MVEA). In this algorithm, the sign bits of the DCT coefficients of Y, C_b, C_r block of I frames and the sign bits of the motion vector in B and P frames were encrypted with one secret key. Inclusion of the motion vector in encryption is very efficient as it significantly degrades the picture quality. Also, the security of this algorithm relies on the length of the key. Like their earlier algorithm, the algorithm suffers from known plaintext and ciphertext attacks. (Mukai and Pradhan, 2011; Singh and Manimegalai, 2012).

Qiao and Nahostedt (1997) proposed an algorithm for video encryption. This algorithm is based on the statistical properties of MPEG video standard and symmetric key algorithm standard to reduce the amount of data that is encrypted. This algorithm divides the video stream input into chunks (a_1, a_2, a_3, …., a_{2n-1}, a2n). The chunks are then divided into two data segments; the odd list (a_1 ,a_3 , …, a_{2n-1}) and even list (a_2,a_4, …a_{2n}). After this, key for encryption is applied to the even list E (a_2, a_4, …a_{2n}) where E denotes an encryption function. The final cipher text is a concatenation of output of encryption algorithm XORed with the odd list streams which makes the technique invulnerable to known-plaintext attack because the key is changed for each frame. (Darshana and Parvindar, 2012; Yogita, 2013)

6. Conclusion

This paper presents a review on the basic concept of video compression and also an extensive survey of Video encryption and its Algorithms. Although, an essential and various quality of encryption of video techniques have been proposed in this study, most of the techniques are vulnerable to cryptanalysis attacks. The total encryption algorithms provide the most secured form of video security but it is computationally expensive and not applicable in real-time applications. Algorithms based on permutation are very fast but they do not provide

meaningful degree of video security. Selective based encryption techniques reduce complexity in computation posed by the naïve video encryption algorithms. They select only few dataset to encrypt videos. The security and speed level is dependent on the part of the video data encrypted. Perceptual encryption algorithms are suitable for applications where the potential video users may need to see a lower quality version of the video before buying them. They are unsuitable for systems that require strong security platform. It is however impossible for a single algorithm to satisfy all performance metric requirements. Thus, selecting an encryption algorithm depends on requirements of the application in use. It can be concluded that it is a challenge for researchers to design an encryption algorithm which maintains tradeoff among all performance parameters.

References

Abomhara, M., Zakaria, O., & Khalifa, O. (2010). An overview of video encryption techniques. In ternational Journal of computer theory and engineering. 2 (1).

Ajay, K., Sourabh, K., Ketki, H., & Aniket, M. (2013). Proposed video encryption algorithm vs other existing algorithms: A comparative study. International Journal of Computer Applications. 65 (1).

Alattar, A.M., Al-Regib, G.I., & Al-Semari, S.A. (1999). Improved selective encryption techniques for secure transmission on MPEG video bit streams. Proceedings of International Conference on Image Processing.

Chiaraluce, F., Ciccarelli, L., Gambi, E., Pierleoni, P., & Reginelli, M. (2002). A new chaotic algorithm for video encryption. Institute of Electrical and Electronics Engineer Transactions on Consumer Electronics. 48 (4). (833-844).

Darshana, H., & Parinder, S. (2012). A comprehensive survey of video encryption algorithms. International Journal of Computer Applications. 59 (1).

Djordje, M. (2009). Video Compression. University 0f Edinburgh. Retrieved via www.google.com.

Eugene, T., Gregory, W. C., Paul, S., & Edward, J. D. An overview of security issues in streaming video. Retrieved via www.google.com.

Furht, B., Muharemagic, E., & Socek, D. (2005). Multimedia encryption and watermarking. Springer-Verlag, New York.

Ganesan, K., Singh, I., & Narian, M. (2008) Public key cryptography of images and videos in real time using chebyshev maps. Proceedings of the 2008 Fifth International Conference on Computer Graphics, Imaging and Visualization, Institute of Electrical and Electronics Engineer Computer Society, Washington DC, USA. (211-216).

Hosseini, M. (2012). A survey of data compression algorithms and their applications. Network Systems Laboratory, School of Computing

Science, Simon Fraser University, BC, Canada.

John, J., & Mamimurugan, S. (2012). A survey on various encryption techniques. International Journal of Soft Computing and Engineering (IJSCE). 2 (1).

Jolly, S., & Vikas, S. (2012). Video encryption: A Survey. International Journal of Computer Science Issues. 8 (2).

Mayank, A. C., Ravindra, P., & Navin, R. (2012). A novel approach of digital video encryption. International Journal of Computer Applications. 49 (4).

Meyer, J., & Gadegast, F. Security mechanism for multimedia data with the example MPEG-1video, project description of SECMPEG.

Mukut, R., & Pradhan, C., (2011). Secured selective encryption algorithm for MPEG-2 video. Journal of Institute of Electrical and Electronics Engineers.

Lelewer, D., & Hirschberg, D. (1987). Data compression. ACM Computing Surveys.

Li, S., Zheng, X., Mou, X., & Cai, Y. (2002). A chaotic encryption scheme for real time digital video. Proceedings of SPIE, SPIE press, San Jose, CA. 149-160.

Rajagopal, S., & Shenbagavalli, A. (2012). A survey of video encryption algorithm implemented in various stages of compression. International Journal of Engineering & Technology (IJERT). 2 (2)

Raymond, W., & Furht, B. (1997). Real-time video compression techniques and algorithms. Kluwer Academic Publishers.

Sashikala, M. Y., Arunodhayan, S.S., & Nachappa, M.N. (2013). A survey of compression techniques. International Journal of Recent Technology and Engineering (IJRTE). 2 (1)

Sayood, K. (2003). Lossless compression handbook. Academic press, 2003.

Shi, C., & Bhargava, B. (1998). A fast MPEG video encryption. Proceedings of the 6th ACM International Conference on Multimedia, New York, USA. (81-88).

Spanos, G.A., & Maples, T.B. (1995). Performance study of a selective encryption scheme for the security of networked, real-time video. In the Proceedings of the 4th International Conference on Computer and Networks (ICCCN '95). (2-10).

Suganya, G., & Mahesh, K. (2014). A survey of various techniques of video compression. International Journal of Engineering Trends and Technology (IJERT). 7(1).

Puech, W., Erkin, Z., Barni, M., Rane, S., & Lagendijk, R. L. (2012). Emerging cryptographic challenges in image and video processing. Journal of Institute of Electrical and Electronics Engineers.

Qiao, L., & Nahrstedt, K. A new algorithm for MPEG video encryption. In the Proceedings of the First International Conference

on Imaging Science, Systems and Technology (CISST'97).

Wong, A., & Bishop, W. (2005). An efficient parallel multi-key encryption of compressed video streams. Department of Electrical and Computer Engineering, University of Waterloo.

Wu, C.P., Kuo, C.C. (2005). Design of integrated multimedia compression and encryption systems. Institute of Electrical and Electronics Engineer Transaction of Multimedia. 7(5). (828-839).

Yan, L., & Main, C. (2009). H.264-Based multiple security levels net video encryption scheme. Institute of Electrical and Electronics Engineers International Conference on Electronic Computer Technology.

Yang, S., & Sun, S. (2008). A video encryption method based on chaotic maps in DCT domain. Progress in Natural Science. 18 (10). (1299-1304)

Yogita, N. (2013). A survey of video encryption techniques. International Journal of Emerging Technology and Advanced Engineering.3 (4).

Zhaopin, S., Guofu, Z., & Jianguo, J. (2012). Multimedia security, a survey of chaos based encryption technology multimedia. School of Computer and Information, Hefei University of Technology, China.