Circuits and Systems, 2016, 7, 1190-1198
Published Online June 2016 in SciRes. http://www.scirp.org/journal/cs
http://dx.doi.org/10.4236/cs.2016.78102

Secured Data Transmission Using Modified LEHS Algorithm in Wireless Sensor Network

C. Bennila Thangammal[1], D. Praveena[2], P. Rangarajan[3]

[1]Department of Electronics & Communication Engineering, R.M.D Engineering College, Chennai, India
[2]Department of Information Technology, R.M.D Engineering College, Chennai, India
[3]Department of Computer Science and Engineering, R.M.D Engineering College, Chennai, India
Email: cbt.it@rmd.ac.in, praveena.it@rmd.ac.in, prr.eee@rmd.ac.in

Received 17 March 2016; accepted 30 May 2016; published 2 June 2016

Abstract

In the ancient block Hill cipher, the cipher text is obtained by multiplying the blocks of the plain text with the key matrix. To strengthen the keymatrix, a double guard Hill cipher was proposed with two key matrices, a private key matrix and its modified key matrix along with permutation. In the ancient block Hill cipher, the cipher text is obtained by multiplying the blocks of the plain text with the key matrix. To strengthen the key matrix, a double guard Hill cipher was proposed with two key matrices, a private key matrix and its modified key matrix along with permutation. In this paper a novel modification is performed to the double guard Hill cipher in order to reduce the number of calculation to obtain the cipher text by using non-square matrices. This modified double guard Hill cipher uses a non-square matrix of order (p × q) as its private keymatrix.

Keywords

Encryption, Decryption, Non-Square Matrices, Low Energy High Secured Data Transmission

1. Introduction

Recent advancement in computer industry, communication and technology leads to an information revolution for past two decades. In information revolution, securing the information is the major issue. Also it throws many unique challenges in transmitting the digital information, a digital data or a multimedia data, through an unsecured wireless network. Cryptology is the science used to secure the information. Cryptology is a Greek word compounded by "kryptos" means hidden and "logos" means word. The study of "cryptology" is called cryptography. The art of sending message secretly was in practice even before four thousand years as a safety measure in military and diplomatic communications.

How to cite this paper: Thangammal, C.B., Praveena, D. and Rangarajan, P. (2016) Secured Data Transmission Using Modified LEHS Algorithm in Wireless Sensor Network. *Circuits and Systems*, **7**, 1190-1198
http://dx.doi.org/10.4236/cs.2016.78102

In cryptography and network security by William stallings, encryption and decryption are the two terms used for secured communication. In encryption, the information which is to be transmitted safely (plaintext) is converted to cipher text using any algorithm or logic. In decryption, the received cipher text is decrypted using the same algorithm or logic used during the encryption to obtain the original information.

Nowadays, the computer ciphers substitute the mechanical cryptology techniques. Many ciphers are formulated with the help of substitution and transposition principles. All the ciphers depend on choosing a key either public or private. Three issues have to be addressed to propose a new cipher. The operations used to convert plaintext to cipher text and cipher text to plaintext are formed meticulously. Then the status of keys used for encryption and decryption as private or public and number of keys used in the process are arrived and the processing of the plaintext had to finalized.

All traditional cryptosystems developed before 1970s are symmetric key cryptosystems. Most of the contemporary cryptosystem are symmetric such as Advanced Encryption Standard [1] (AES), Data Encryption Standard [2] (DES), RC5 [3], Hill Cipher [4], and many more. Hill cipher is a classical symmetric block cipher utilized in different ways according to the applications and it is also possible to encrypt and validate the information at the same time. It can be intended to have high speed of ciphering and deciphering with high data throughput [5]. Also, Hill cipher has a weak security cryptosystem due to the linearity property and it is vulnerable to known-plaintext attack.

In Hill cipher alphabets, A to Z was masked with the values of 0 to 25 and ciphered using private key matrix. Hill cipher is capable of encrypting alphabets alone not the numerals and special characters. It is susceptible to “Known Plain text attack” as the key matrix is not permutated. To conquer this security flaw, many researchers proposed the unique modification. Ismail *et al.* [6] proposed a modified Hill cipher named HILLMRIV algorithm, a secret initial vector is used to obtain the unique key for enciphering. Rangel-Romero *et al*. [7] claimed that HILLMRIV algorithm has few major drawbacks and it is still prone to Known-plaintext attacks.

V. U. K. Sastry *et al.* [8]-[10] customized the original Hill cipher by including interweaving, interlacing and iteration. Modified Hill cipher [8] [9] have avalanche effect and are believed to defend against any cryptanalytic attack. Many of the modifications such as how the interweaving and interlacing along with the iteration will strengthen the Hill cipher and the necessity of the number of iteration to be 16 are not argued. The crisis of non-invertible key matrix in Hill cipher is addressed by Rushdi *et al.* [11]. The key problem is resolved by translating each character of the plaintext to two cipher text characters but the computational complexity and duration is increased. Bibhudendra *et al.* [12] proposed AdvHill (Advanced Hill) algorithm to address the non-invertible matrix key issue by involving involutory matrix key for enciphering. The computational complexity is reduced by removing the inverse key calculation process in AdvHill algorithm.

Many researches are performed to improve the security flaws in Hill cipher by strengthening the key matrix. To prevent the vulnerability against the known plaintext attack Yeh *et al.* [13] make use of securely shared two co-prime numbers between the communication parties. Even though it reaches its basic objective it cannot be efficiently used for a bulk of data as it is time consuming and need many mathematical manipulations. Saeednia [14] proposed a secured Hill cipher by permuting the rows and columns of the key matrix randomly, still it is vulnerable to known plaintext attack. Once again V. U. K. Sastry *et al.* [15] modified the Hill cipher by masking the letters using Extended Binary Coded Decimal Interchange Code (EBCDIC) to support IBM mainframes. But it is not suitable energy constrained networks as the iteration process of the data is performed bit wise. In order to strengthen the Hill cipher the key dependent permutation and interlacing is used for large block size of the plain text in [16]. Again to make the cipher stronger author combined the modified Hill cipher with playfair cipher [17].

Hill cipher is modified using Maximum Distance Separable (MDS) variable length key matrix to strengthen the security of the cryptosystem [18]. The security level of the cryptosystem is strengthen by modifying the private key matrix of the Hill cipher and proposed a double guard Hill cipher [19]. It supports ASCII values and the private key matrix is permutated to triumph over the known plaintext attack. Also, double protection is given to the cryptosystem by shuffling the enciphered text with respect to “t” matrix before transmitting so that it can overcome chosen plaintext attack, cipher text attack as well as chosen cipher text attack. Images can be transmitted energy efficiently in a secured manner by combining Losningen cross layer approach with the double guard Hill cipher algorithm (DGHC) in [20]. Further, the energy consumption can be reduced by reducing the computational time and by reducing the number of bits to be transmitted. In order to reduce the computation time efficiently, the number of calculation can be reduced to minimize the energy consumed in the proposed modified Double Guard Hill cipher (MDGHC).

2. A Modified Double Guard Hill Cipher with Non Square Matrix

The Double Guard Hill Cipher is modified with the non-square key matrix of the order (p × q) and the message matrix is obtained with respect to the values of p and q of key matrix. This novel modification is performed expecting to reduce the computational time and the number of bits transmitted. The permutation procedure is replaced by simply exchanging either rows or columns without changing its determinant. The encryption and decryption algorithm of the proposed modified double guard Hill cipher is

2.1. Encryption Algorithm

The encryption algorithm (**Figure 1**) to convert the plaintext into cipher text is

1) Let [*K*] by the non-square key matrix of $p \times q$. If $p > q$, it is called as vertical matrix else it is horizontal matrix.

2) The message matrix [*M*] is arranged according the key matrix [*K*].
For vertical key matrix: order of the message matrix [*M*] is $q \times n$.
For horizontal key matrix: order of the message matrix [*M*] is $m \times p$.

3) Obtain the encrypted cipher matrix [*C*] by
For vertical key matrix:

$$[C]=[K]\cdot[M] \tag{1}$$

For horizontal key matrix:

$$[C]=[M]\cdot[K] \tag{2}$$

Note: In a non-square matrix, two matrix [*A*] and [*B*] of different order is not associative.

4) Before transmitting, the rows and columns are interchanged so that it is prone to various attacks like "known plain text attack", "chosen plain text attack", "cipher text attack" as well as "chosen cipher text attack".

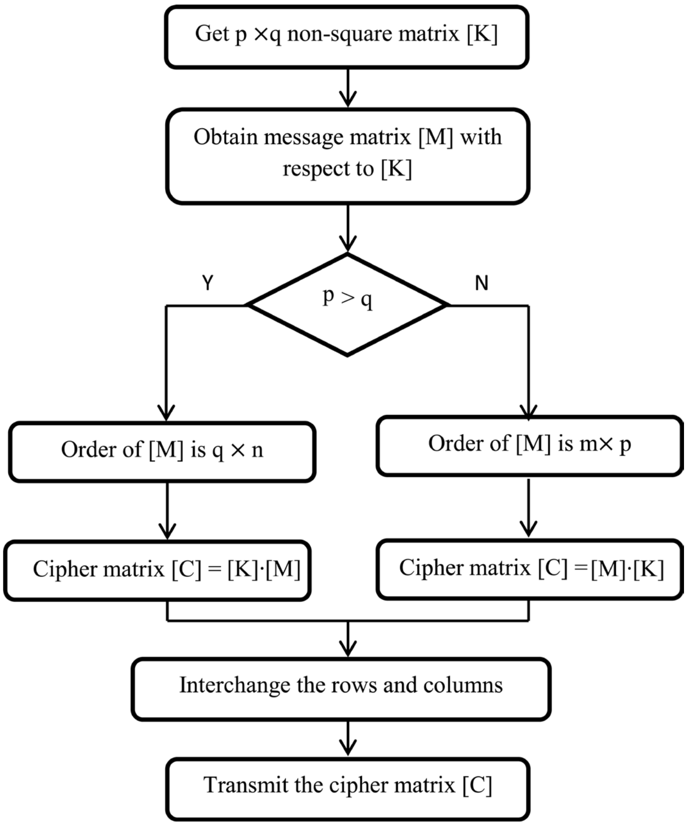
Get p ×q non-square matrix [K]
Obtain message matrix [M] with respect to [K]
p > q
Y
N
Order of [M] is q × n
Order of [M] is m× p
Cipher matrix [C] = [K]·[M]
Cipher matrix [C] =[M]·[K]
Interchange the rows and columns
Transmit the cipher matrix [C]

Figure 1. Encryption algorithm of modified double guard hill cipher.

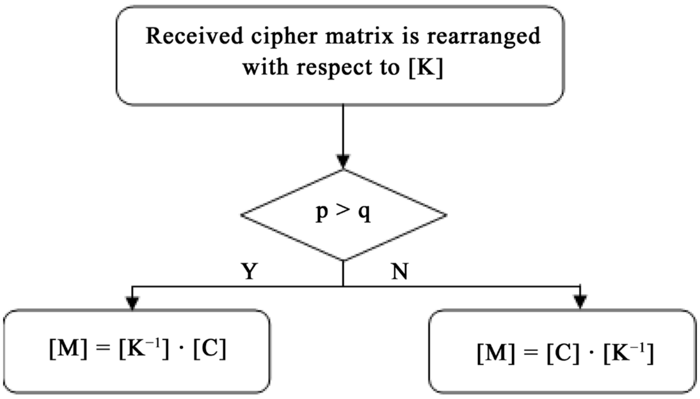

Figure 2. Decryption algorithm of modified double guard hill cipher.

Thus the encrypted matrix is obtained for transmission. As the permutation of the key matrix is not performed, there is no need to transmit the "*t*" matrix along with the encrypted matrix.

2.2. Decryption Algorithm

The decryption algorithm (**Figure 2**) to convert the cipher text to the plaintext is

1) Received encrypted matrix is rearranged with respect to the key matrix.
2) Plain text is obtained by multiplying the Mod-128 inverse key with the rearranged encryption matrix.

For vertical key matrix,

$$[M]=\left[K^{-1}\right]\cdot[C] \tag{3}$$

For horizontal key matrix,

$$[M]=[C]\cdot\left[K^{-1}\right] \tag{4}$$

Note: According to theorem 1 [21], right inverse exist for horizontal matrix and left inverse exist for vertical matrix.

Theorem 1

Every non singular horizontal matrix A having a right inverse A_R^{-1} *such that*

$$A_R^{-1}=\frac{1}{|A|}adj(A)$$

2.3. Illustration of Proposed Modified Double Guard Hill Cipher

The modified Double Guard Hill Cipher is illustrated with a sample message as

Message: "**Meet on 3-3@ #R**"

ASCII value: [77 101 101 116 32 111 110 32 51 45 51 64 35 82]

Encryption for vertical key matrix:

Key matrix of order 4 × 3: $[K]=\begin{bmatrix}1 & 20 & 13\\ 34 & 3 & 8\\ 57 & 65 & 73\\ 14 & 3 & 9\end{bmatrix}$

Since the message matrix should have 3 × *n*, it is arranged to 3 × 5 for the given key matrix. Arrange [*M*] column wise

$$[M]=\begin{bmatrix}M & t & n & - & \#\\ e & \text{ƀ} & \text{ƀ} & 3 & R\\ e & o & 3 & @ & 0\end{bmatrix}$$

$$[M]=\begin{bmatrix}77 & 116 & 110 & 45 & 35\\ 101 & 32 & 32 & 51 & 82\\ 101 & 111 & 51 & 64 & 0\end{bmatrix}$$

$$[C]=[K]\cdot[M]$$

$$[C]=\begin{bmatrix}1 & 20 & 13\\ 34 & 3 & 8\\ 57 & 65 & 73\\ 14 & 3 & 9\end{bmatrix}\times\begin{bmatrix}77 & 116 & 110 & 45 & 35\\ 101 & 32 & 32 & 51 & 82\\ 101 & 111 & 51 & 64 & 0\end{bmatrix}$$

$$[C]=\begin{bmatrix}82 & 23 & 5 & 105 & 11\\ 17 & 64 & 20 & 19 & 28\\ 23 & 27 & 41 & 56 & 29\\ 114 & 31 & 47 & 79 & 96\end{bmatrix}$$

$$[C]=\begin{bmatrix}82 & 17 & 23 & 114\\ 23 & 64 & 27 & 31\\ 5 & 20 & 41 & 47\\ 105 & 19 & 56 & 79\\ 11 & 28 & 29 & 96\end{bmatrix}$$

The encrypted matrix in row wise,

[*C*] = [82 17 23 114 23 64 20 19 28 23 27 41 56 29 114 31 47 79 96] is transmitted.

Decryption for vertical key matrix:

The received encrypted cipher matrix is rearranged column wise with respect to the column of mod-128 inverse of the key matrix, [K^{-1}]

$$[C]=\begin{bmatrix}82 & 23 & 5 & 105 & 11\\ 17 & 64 & 20 & 19 & 28\\ 23 & 27 & 41 & 56 & 29\\ 114 & 31 & 47 & 79 & 96\end{bmatrix}$$

Note: The determinant of the non-square matrix is obtained by using the Theorem 2 and the modulo inverse of the non-square matrix is obtained by Theorem 3.

Theorem 2

The determinant of a non-square matrix is given as

$$\textit{If}\quad A=\begin{bmatrix}a_{11} & a_{12} & \cdots & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & \cdots & a_{2n}\end{bmatrix}\quad \textit{then its}\quad |A|=\sum_{i=1}^{n-1}\sum_{j=i+1}^{n}(-1)^{P_{ij}}\begin{vmatrix}a_{1i} & a_{1j}\\ a_{2i} & a_{2j}\end{vmatrix}$$

$$\textit{If}\quad A=\begin{bmatrix}a_{11} & a_{12}\\ a_{12} & a_{22}\\ \vdots & \vdots\\ \vdots & \vdots\\ a_{n1} & a_{n2}\end{bmatrix}\quad \textit{then its}\quad |A|=\sum\nolimits_{i=1}^{n-1}\sum\nolimits_{j=i+1}^{n}(-1)^{P_{ij}}\begin{vmatrix}a_{i1} & a_{j1}\\ a_{i2} & a_{j2}\end{vmatrix},\quad \textit{where}$$

$$P_{ij}=\begin{cases} j-\dfrac{i}{2}+\dfrac{(-1)^i}{4}+\dfrac{3}{4};\ \text{if } n \text{ is even}\\ j-\dfrac{i}{2}-\dfrac{(-1)^i}{4}+\dfrac{9}{4};\ \text{if } n \text{ is odd}\end{cases}$$

Theorem 3

Inverse of the non-square matrix is given by

$A^{-1} = \frac{1}{|A|} adj(A)$ *where cofactor is given by* $A_{ij} = (-1)^{i+j} M_{ij}$, M_{ij} *is minor of* A_{ij}.

The mod-128 inverse of the key matrix [*K*] is

$$[K^{-1}] = \begin{bmatrix} 2 & 72 & 113 & 69 \\ 75 & 108 & 29 & 44 \\ 114 & 31 & 47 & 96 \end{bmatrix}$$

$$[M] = [K^{-1}] \cdot [E] = \begin{bmatrix} 2 & 72 & 113 & 69 \\ 75 & 108 & 29 & 44 \\ 114 & 31 & 47 & 96 \end{bmatrix} \times \begin{bmatrix} 82 & 23 & 5 & 105 & 11 \\ 17 & 64 & 20 & 19 & 28 \\ 23 & 27 & 41 & 56 & 29 \\ 114 & 31 & 47 & 79 & 96 \end{bmatrix}$$

$$[M] = \begin{bmatrix} 77 & 116 & 110 & 45 & 35 \\ 101 & 32 & 32 & 51 & 82 \\ 101 & 111 & 51 & 64 & 0 \end{bmatrix}$$

$$[M] = \begin{bmatrix} M & t & n & - & \# \\ e & \not{b} & \not{b} & 3 & R \\ e & o & 3 & @ & 0 \end{bmatrix}$$

Similarly the encryption and decryption for horizontal key matrix can be performed.

The cipher text obtained by using the vertical key matrix and horizontal key matrix are different for the same plaintext. Similarly, according to the non-square matrix theorem, right inverse matrix exist for the horizontal matrix and left inverse matrix exist for the vertical matrix. The original plaintext cannot be retrieved if the inverse matrices are multiplied reversely.

In the modified double guard Hill cipher the encryption time is reduced as it avoid the permutation and the transmitted are reduced as it avoids the transmission of 'U' matrix along with the cipher text. The execution time and the encryption speed (**Table 1**) of the modified double guard Hill cipher is compared with large block cipher involving key dependent permutation, interlacing and iteration, block cipher with the blending of Hill cipher and playfair cipher, double guard Hill cipher and the contemporary ciphers such as DES and AES.

The proposed cipher is strengthened against the 'known plaintext attack' without the procedure of permutation by the property of non-square matrix and shuffling the order of the cipher text. The transmission of 'U' matrix along with encrypted cipher text in double guard Hill cipher is eluded by evading permutation. So, in the modified double guard Hill cipher the encryption time is reduced by reducing the number of computation, also it reduce the bits transmitted when compared with double guard Hill cipher. The proposed cipher is capable of encrypting the data faster than the various ciphers.

Table 1. Comparison of encryption speed and execution time of the proposed cipher with other ciphers.

Cipher	Execution time of Encryption/Bytes in ms	Length of plain text in binary	Length of key in binary	Encryption Bytes/Second
DES	31.1/320	64	56	7988
AES	61.2/320	128	128	5320
Block cipher with blending of Hill cipher and playfair cipher	11.5/288	112	448	25,043
Large block cipher involving key dependent permutation, interlacing and iteration	8.5/256	448	384	30,608
A double guard Hill cipher	6.12/256	448	288	32,520
Modified Double guard Hill cipher	5.4/256	448	384	37,224

3. Secured Data Transmission Using Modified LEHS

In Wireless Sensor Network (WSN), data can be securely transmitted in an energy efficient manner using modified LEHS (Low Energy High Secured) algorithm. In modified LEHS algorithm, the backbone of the network to transmit the data to the base station is configured by Losningen cross-layer approach (LCA) to enable the energy efficient transmission in order to enhance the network's lifetime and the data is secured using modified Double Guard Hill cipher. Losningen approach [22] merges the MAC layer, sublayer of the data link layer, with network layer. Normally for various services and protocols, the lowest layers of the system were used maximally to pass information to the higher layers. So the cross layered approach of merging MAC layer with network layer is carried out to obtain the information about the link quality and the congestion from the MAC layer when routing is performed. This achieves the energy efficiency by balancing the network traffic that limits the queuing delay and packet loss due to the traffic. So, the objective of enhancing the network's lifetime with reasonable delay and throughput is obtained by implementing the cross layer approach for routing. This approach will provide the overall view of underlying information to the routing layer for choosing the better path.

Routing performance can be increased enormously by this approach as the link quality and the congestion information are revealed to network layer immediately. The cross-layer designs with tight coupling between many layers become hard to review and redesign. Since changing one subsystem leads to changing of all other parts because of interconnection. Hence in Losningen cross layer approach, the merging of MAC layer with the network layer preserves the modularity of the network to ease the review and redesign for the future enhancement.

An earnest effort has been made to develop the cross layer approach [20] that improves the throughput by 1.7 times higher than the network without cross layer approach with AODV routing protocol. Network's lifetime is prolonged by 1.2 times more by the proposed approach. It is achieved by reducing 42% of data packet loss. The end-to-end delay is reduced by the factor of 1.5 by reducing the delays caused by route discovery, queuing delay at network interface and retransmission delays due to the transmission of data from source to sink.

At the network layer, the traffic is balanced through the AOMDV routing protocol. AOMDV routing protocol allows significant energy conservation as it has the ability to reduce the route discovery frequency. This routing algorithm is on-demand algorithm that enables self-starting, dynamic, multihop routing when a source node wants to send a data packet. Since the routing messages are of small fixed length packets and uses it on-demand basis, it suits well for WSNs. As it is capable of providing multiple redundant paths, the data can be transferred using alternate path during path failure.

The three main phases of this algorithm are route discovery, route updation and route re-establishment. When a node wants to transmit a data to another node without prior knowledge of the destination, it enables the route discovery phase by flooding the route request (RREQ) in order to notify the destination of the data packet. To minimize the energy required for flooding, the length of the request is small and constant.

The propagation of RREQ from the source to the sink (destination) node launches multiple reverse paths at the intermediate nodes as well as the destination nodes. The frequency of route discovery is reduced as the AOMDV routing protocol provides the alternate paths for the intermediate nodes too. The destination node responds to the first received request and discards the duplicate ones. It sends the route reply (RREP) back to the source node on the fastest route called on-route nodes. This routing protocol establishes and maintains efficient routes in dynamic topology. When the routes are disconnected, the routing protocol makes use of local topology information gathered by the medium access protocol to re-establish the route efficiently.

Performance of the modified LEHS algorithm for data transmission is simulated using network simulator-2 (NS2). Simulation results are obtained by considering maximum of 100 nodes randomly deployed in a uniform rectangular field of dimension 1000 m × 1000 m. Traffic pattern between the chosen source sink pair consist of several CBR/UDP connections. Let the packet size be 500 bytes and the number of packets transmitted per second be 25 with the packet transfer interval time of 0.04 seconds.

The metric used to evaluate the performance is network lifetime. Network lifetime measures the amount of time before a certain percentage of sensor nodes run out of battery power. During the simulation, the whole network is considered to be down when 25% of the normal sensor nodes are depleted of power. The simulation result of modified LEHS algorithm for data transmission is compared with LEHS algorithm with DGHC in order to prove the enhancement of network's lifetime. From the readings, the network lifetime of LEHS-MDGHC is seems to be enhanced by 2.4 times than LEHS-DGHC as shown by **Figure 3**.

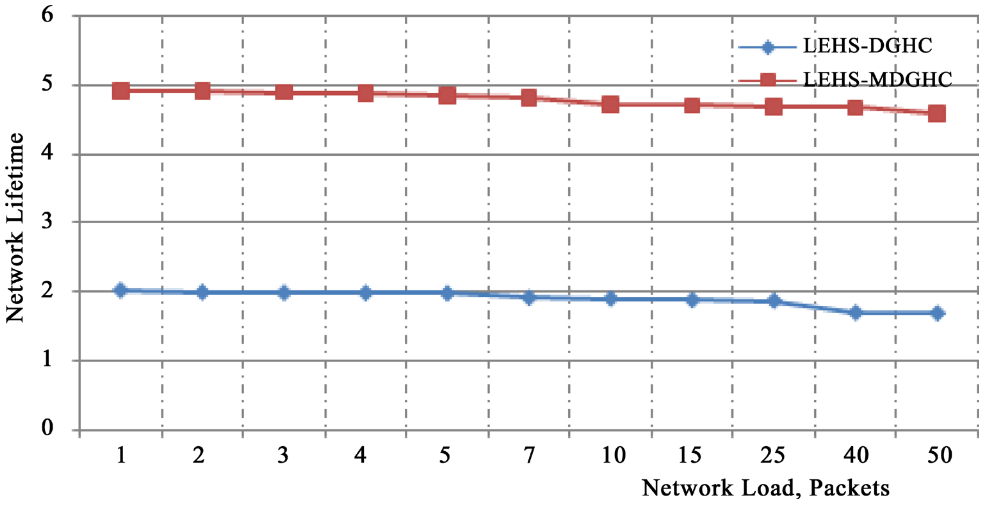

Figure 3. Comparison of network lifetime between LEHS-DGHC and LEHS-MDHGC.

4. Conclusion

In the modified double guard Hill cipher, the non-square matrices are used as private key matrix. Because of the property of non-square matrix and obtaining the cipher text by twisting the order of the cipher text strengthen the proposed cipher against the "known plaintext attack" without the procedure of permutation. Also by avoiding permutation, the transmission of "U" matrix along with encrypted cipher text in double guard Hill cipher is eluded. So, in the modified double guard Hill cipher the number of computation is reduced by avoiding the permutation, also it reduce the bits transmitted when compared with double guard Hill cipher. The proposed cipher is capable of encrypting the data faster than the various ciphers. Therefore in future, it can be refined for image encryption in wireless sensor network in order to enhance the network's lifetime for secure image transmission.

References

[1] Daemen, J. and Rijmen, V. (2001) Rijndael: The Advanced Encryption (AES). *Dr. Dobb's Journal*, **26**, 137-139.

[2] Coppersmith, D. (1994) The Data Encryption Standards and Its Strength against Attacks. *IBM Journal of Research and Development*, **38**, 243-250. http://dx.doi.org/10.1147/rd.383.0243

[3] Rivest, R.L. (1995) The RC5 Encryption Algorithm. *Dr. Dobb's Journal*, **20**, 146-148.

[4] Hill, L. (1929) Cryptography in an Algebraic Alphabet. *The American Mathematical Monthly*, **36**, 306-312. http://dx.doi.org/10.2307/2298294

[5] Overbey, J., Traves, W. and Wojdylo, J. (2005) On the Keyspace of the Hill Cipher. *Cryptologia*, **29**, 59-72. http://dx.doi.org/10.1080/0161-110591893771

[6] Ismail, I.A., Amin, M. and Diab, H. (2006) How to Repair the Hill Cipher. *Journal of Zhejiang University Science A*, **7**, 2022-2030. http://dx.doi.org/10.1631/jzus.2006.A2022

[7] Rangel-Romero, Y., Vega-García, G., Menchaca-Méndez, A., Acoltzi-Cervantes, D., Martínez-Ramos, L., Mecate-Zambrano, M., Montalvo-Lezama, F., Barrón-Vidales, J., Cortez-Duarte, N. and Rodríguez-Henríquez, F. (2008) Comments on How to Repair the Hill Cipher. *Journal of Zhejiang University Science A*, **9**, 211-214. http://dx.doi.org/10.1631/jzus.A072143

[8] Sastry, V.U.K. and Ravi Shankar, V. (2007) Modified Hill Cipher with Interlacing and Iteration. *Journal of Computer Science*, **3**, 854-859. http://dx.doi.org/10.3844/jcssp.2007.854.859

[9] Sastry, V.U.K., Ravi Shankar, N. and Durga Bhavani, S. (2010) A Modified Hill Cipher Involving Interweaving and Iteration. *International Journal of Network Security*, **10**, 210-215.

[10] Sastry, V.U.K,. Ravi Shankar, N. and Durga Bhavani, S. (2013) A Large Block Cipher Involving Key Dependent Permutation, Interlacing and Iteration. *Bulgarian Academy of Sciences*, **13**, 50-63.

[11] Rushdi, A.H. and Mousa, F. (2009) Design of a Robust Cryptosystem Algorithm for Non-Invertible Matrices Based on Hill Cipher. *International Journal of Computer Science and Network Security*, **9**, 11-16.

[12] Acharya, B., Rath, G.S. and Patra, S.K. (2008) Novel Modified Hill Cipher Algorithm. *Proceedings of ICETAETS*, 126-130.

[13] Yeh, Y.S., Wu, T.C., Chang, C.C. and Yang, W.C. (1991) A New Cryptosystem Using Matrix Transformation. *Proceedings of the* 25*th IEEE International Carnahan Conference on Security Technology*, Taipei, 1-3 October 1991, 131-138. http://dx.doi.org/10.1109/ccst.1991.202204

[14] Saeednia, S. (2000) How to Make the Hill Cipher Secure. *Cryptologia Journal*, **24**, 353-360. http://dx.doi.org/10.1080/0161119000898425З

[15] Sastry&Janaki (2007) A Block Cipher Using Linear Congruences. *Journal of Computer Science*, *Science Publications*, **3**, 556-561.

[16] Sastry, V.U.K., Varanasi, A. and Udaya Kumar, S. (2011) A Modern Advanced Hill Cipher Involving a Permuted Key and Modular Arithmetic Addition Operation. *Journal of Global Research in Computer Science*, **2**, 92-96.

[17] Sastry, V.U.K., Ravi Shankar, N. and Durga Bhavani, S. (2011) A Blending of A Generalized Playfair Cipher and A Modified Hill Cipher. *International Journal of Networks and Mobile Technology*, **2**, 35-43.

[18] Magamba, K., Kadaleka, S. and Kasambara, A. (2012) Variable length Hill Cipher with MDS Key Matrix. *International Journal of Computer Applications*, **57**, 43-45.

[19] Thangammal, C.B., Rangarajan, P. and Raja Paul Perinbam, J. (2013), A Double Guard Hill cipher suitable for Wireless Sensor Networks. *Journal of Theoretical and Applied Information Technology*, **57**, 1-6.

[20] Bennila Thangammal, C., Rangarajan, P. and Raja Paul Perinbam, J. (2014) Secured Image Transmission Using LEHS Algorithm in Wireless Sensor Network to Enhance the Network's Life-Time. *Comptesrendus de l'Academia bulgare des Sciences*, **67**, 1401-1410.

[21] Ganapathy, M. and Kumar, A. (2011) Determinant for Non-Square Matrices. *International Journal of Mathematical Sciences and Engineering Applications*, **5**, 1-13.

[22] Bennila Thangammal, C., Rangarajan, P. and Raja Paul Perinbam, J. (2012) Maximization of Wireless Sensor Network's Lifetime Using Losningen Cross-Layer Approach. *Asian Journal of Scientific Research*, **5**, 133-142. http://dx.doi.org/10.3923/ajsr.2012.133.142