VOL. 10, NO. 5, MARCH 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

ADAPTIVE MODULATION WITH MULTI-LEVEL SECURITY USING SPARSE MATRICES

Navaneethan C.[1] and K. Helen Prabha[2]
[1]Anna University, India
[2]R.M.D Engineering College, Tamil Nadu, India
E-Mail: c.navaneethan16@gmail.com

ABSTRACT

In the wireless sensor network system, wide ranges of techniques have been developed for securing the data before transferring to the concerned destination. Cryptography and modulation are distinct techniques that are used in wide range to protect the information from the attackers. In this slog we came up with a work of "Adaptive Modulation with Multi-Level Security for Networks", in which the plain text is encrypted by using the newly proposed Encryption and Decryption Based on Sparse Matrices algorithm. This algorithm is a multi-staged encryption and decryption. By deploying encryption algorithm at the sender side message is encrypted before operating with modulation and demodulation algorithm. Encrypted message is then modulated through modulator. At the receiver side demodulation is performed followed by decryption operation. This approach results in the secure adoption of modulation with effective cryptography in unsecured channel more effectively.

Index terms: modulation, demodulation, cryptography, sparse matrices.

1. INTRODUCTION

Wireless sensor network (WSN) has distinct features of extracting data and providing communication between edges of the world through different medium by using sensor nodes. Each node has properties to achieve the impetus to which the resources should be considered as a barren.

The network ensures that there is a overhead on the sensor node in its process of operation, in which increasing the system efficiency with longer period is the major concern. This can be achieved by incorporating different techniques of diffusion, clustering, adoption of different cryptographic algorithms, which consumes fewer resources.

Although, there is significant research on energy efficient WSNs, security is major concern for network. As it doesn't matter how data is transferring, and matters how securely it is transferring, there is always need of new techniques to be employed to achieve secrecy. To be in race a lot of techniques are emerged. The archetypal techniques are modulation, Encryption/ decryption with and without keys, and many other cryptographic algorithms. The need of Encryption and modulation changed the mode of data transfer through networks.

1.1 Adaptive modulation

The adaptive modulation is used in a centralized cross-layer approach in order to minimize the total transmission energy consumption of a network. Every node in the group is adjusted to have a different bit rate according to its application. In this technique, one common modulation scheme is considered depending on the channel conditions across the network to achieve lower required energy per bit.

1.1.1 Objective

The objectives of the framework includes factors as mentioned

a) Switching between modulation and demodulation of different approaches for a node.
b) Maintaining the uniform SNR (Signal to Noise Ratio) by choosing a particular modulation.
c) Automatically extracting the features of the system and identifying the relevant demodulator at receiver by filtering the channel noise.
d) Ensuring security by employing the advanced security standards through multilevel security providing algorithms.

The modulation and demodulation schemes that can be vividly employed includes,

i. Amplitude Shift Keying (ASK) Modulation
ii. Differential 8-ary Phase Shift Keying (D8PSK)
iii. Continuous Phase Frequency Shift Keying (CPFSK)
iv. Eight symbol Quadrature Amplitude modulation (QAM8)
v. Quadrature Amplitude Shift Keying (QASK)
vi. Differential Quadrature Phase Shift Keying (DQPSK)
vii. Sunde Modulation
viii. Quadrature Amplitude modulation (QAM 16)
ix. Quadrature Amplitude modulation (QAM 64)
x. Quadrature Amplitude modulation (QAM 256)

1.2 MULTI-level cryptography with sparse matrices

Cryptographic algorithms are used to provide secure communication between networks. The coding and decoding of information through encryption/decryption algorithm is based on mathematical techniques. Cryptographic algorithm deals with the problems of analyzing and planning of ciphers, that provides secure communications. In general cryptographic algorithm is about designing and analysis of protocols that relates to

various aspects of information security. A strong cryptographic system should be computationally fast, generating randomness, greater resistance to attacks and it must be difficult to decode by the intruders even though the characteristics of algorithm are known.

Here we introduced a cipher which is based on a non-linear transform of Sparse product of matrix $W^m = P^m U^m$, where P^m is a diagonal matrix and U^m is a sparse matrix with a small number of non-zero elements. This matrix is also invertible matrix. By this on finite data we can provide multi-scale analysis and also reveal local information.

Here we proposed a cipher which is based on sparse product of matrix U^m. The procedure includes encryption of a plain text p into a cipher text t_n through a onetime key called P^m and a non-linear transformation which is derived from Sparse product of matrix W^m.

2. CONSTRUCTION OF SPARSE MATRICES

Consider $M_{n,m}$ is the set of all matrices that are of n×m size over the field of complex numbers. If n = m then $M_{n,m}$ is denoted as M_n. The symbol " A = [A_{ij}] " denotes a matrix A with elements A_{ij} and $A_i = \{A_{i,j}: j = 1, \ldots, m\}$ is used to denote the i^{th} row of a matrix A $\in M_{n,m}$. The support of the row A_i is: supp{Ai} ={j = 1, .., m : Aij ≠ 0}. A^T denotes the transpose of a matrix 'A'. A square matrix A ∈Mn is said to be invertible if only if there is an unique square matrix A∈M_n which is called as inverse matrix of A such that A $A^{-1} = I_n$, where I_n is the identity matrix.

The ceiling of a real number x be denoted as $\lceil x \rceil$: inf{n∈ Z:x≤n}(where Z is a set of integers). If p and q are any natural numbers, we denote by Mod (p,q), the remainder on division of p by q and we use the symbol $[q]_p$ = {q+tp: t∈ Z} to denote the residue class of q modulo p.

Consider the unique prime factorization of a positive integer m (up to rearrangement of factors):
$m = p_1 p_2 .. p_N$

$J(0) = 1, J(n) = \prod_{i=1}^{N} p_i$

$A(i) = \prod_{r=i}^{N} p_r$, i = 1,….,N, A(N+1) = 1,
Where $p_1 \geq p_2 \geq .. \geq p_N$ and A(i), J(n) are the partial products of positive integer m.

The following main matrix operators are defined on the set $M_{n,m}$ with some additional matrix operations excluded in the definitions, where p=2,3,….

Prime factorization definition

Let D_p: $M_{n,m} \rightarrow M_{n,pm}$ such that :

$D_p(M)=\{M_{i,\lceil \frac{j}{p} \rceil}, i=1,\ldots,n,\ j=1,\ldots,pm\}$

Definition for deriving sequence of block matrices

We consider the prime factorization of a positive integer m and we define a sequence of block matrices $Um^{(n)} \in M_{J(n)}$, where n = 0, ...,N, by using the following iteration:

$$U^m(n) = \begin{cases} \{1\} & n = 0 \\ S(D_{p1}(Um(0)), R(1,p1)) & n = 1 \\ S(D_{pn}(Um(n-1)), R(J(n-1),pn)) & n = 2,\ldots,N \end{cases}$$

If n=N then we will write $U^m(N) = U^m$.

Product of matrices definition

Let $\{p_1, \ldots, p_m\}$ be the set of prime numbers where m is a positive integer. Consider a diagonal matrix contains elements $\{p_1, \ldots, p_m\}$. Now we define W^m to be the product of matrices P^m and U^m and represented as $W^m = P^m U^m$.

Consider the following sparse matrices:

Here we can see examples of sparse matrices. Here we shown one example, Consider

M = 12= p1, p2, p3 where p1 = 3, p2 = 2, p3 = 2, then N = 3 and we have:

$$U^{12}(1) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

$$U^{12}(2) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix},$$

$$U^{12}(3) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Sparse Matrix with M=12 & N=3

Now, let j=1,….p_n-1,we define the following column matrices $V_j^{p_n} = \{ V_{kj}^{p_n} : k=1,\ldots p_n \}$.

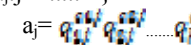
$$V_{kj}^{p_n} = \begin{cases} 1, & whenever\ k = j \\ -1, & whenever\ k = p_n \\ 0, & elsewhere \end{cases}$$

3. ENCRYPTION/DECRYPTION USING SPARSE MATRIX

We have proposed a cipher based on the non linear transform of the sparse product of the matrix W^m that we have introduced above.

We consider a sequence of positive integers

$\alpha=\{\alpha_j:j=1.....m\}$

Let $a_j=$  , j=1.....m

Be the prime factorization of the above numbers. The sequence $\alpha=\{a_j:n=1....m\}$ is the plaintext of our cipher.

The encryption algorithm of the plain text α is the following:

1) Choose an integer
   $N_0 = MAX\ \{c_{ij}:i=1.....k\ ,j=1.....m\} + 1$
   and we select randomly a collection $\{p_1.....p_m\}$ of m various prime numbers that are not equal with the prime
   factors $\{q_{11},q_{21}.....q_{k1,1}\}$ of all the positive integer α_1

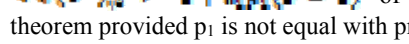
2) Select the matrix U^m and we consider it to be the public
   key of our algorithm. We define the matrix W^m, where the
   diagonal matrix P^m has elements $\{p_1^{N_0}.....p_m^{N_0}\}$.the matrix
   P^m is the private key of our algorithm.

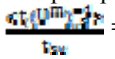
3) Compute the sparse product of the matrix W^m:
   $T_n=\pi_{k=1}^{m}(1+\alpha_k p_k^{N_0} U_{kn}^{m})$
   The sequence $\{t_n=n=1,.....m\}$ is the cipher text of our algorithm.

The Decryption algorithm is as follows:

a) Compute the sequences
   (i) assign $x_1=t_n(t_n=max)$
   (ii) $x_{n+1}=t_{n+1}-x_1$ (n!=0)

b) Calculate the prime factorization of each xi where i=1,2,...m

c) Compute p1 and n0 from the relation
    of
   theorem provided p_1 is not equal with prime factors.

d) Compute prime numbers (p2.....pm) from the equation
    $= a_s p_s^{n_0}\ (S > 1)$
   and from the definition of N_0.

e) Calculate
   (i) $\alpha_s =$  (if s=1)
   (ii) $\alpha_s=$  (if s>1)
   We get the plain text α_i(i=1,2,3.....m)

Example

Let us consider that we want to send the message a = {12, 14, 16, 18, 20} through an non safe communication channel.

The encryption technique of the plaintext a is:

(1) Choose N_0= 3 and we select five random prime numbers:
    {3, 7, 11, 17, 19}.
(2) Select the matrix U^5 and we define the matrix $W^5=P^5U^5$, where P^5 has the elements {27, 343, 1331, 4193, 6859}.
(3) Compute the Sparse product of the matrix W^5 to be:
    t_1= 1560975,t_2= 6921525, t_3= 28741375,
    t_4= 44583825, t_5= 325.

The decryption technique of the cipher text t is:

a) Compute the sequence X_1= 325,X_2= 1560650, X_3= 6921200, X_4 = 28741050, X_5= 44583500.
b) Consider the prime factorizations of $X_2,\ldots,X_5$.
c) Identify that p_1= 3 and N_0= 3, since X_1- 1 = 12*3^3.
d) Identify the rest of the prime numbers of the private key P^m :
   X_2= 2*7*7*7*7*325
   X_3= 2*2*2*2*11*11*11*325,
   X_4=2*9*17*17*17*325,
   X_5 = 2*2*5*19*19*19*325.
e) Compute the plaintext by using decryption formulae:
   α_1=12,α_2=14,α_3=16,α_4=18,α_5=20

The following are the advantages of the proposed algorithm:

a) It is asymmetric.
b) It is realized with the use of non-linear transform.
c) The encryption algorithm is based on prime numbers that are randomly selected.
d) The private key P^m is a one-time key as it is used to encrypt plain text. Also this is an auto key which is difficult for an intruder to find the key.
e) In decryption the cipher is decrypted thrice which is difficult to decode for an intruder.

4. SYSTEM IMPLEMENTATION

The system proposed is implemented in four phases two at the sender end and two at the receiver end. The over all architecture of the system is illustrated in the Figure shown below.

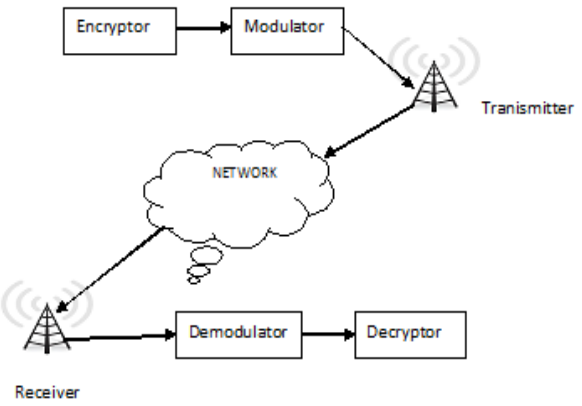


Figure-1. Overall architecture of the system.

At sender side data to be sent undergoes encryption and modulation and then sent through network by using transmitter. Receiver receives the signal and then process that for demodulation followed by decryption.

System configuration of minimum 1GB RAM and 100GB storage capacity with a high-levl technical computing language and interactive environment for algorithm development, data visualization, data analysis are the pre-requisites required on both sides.

5. RESULTS

The proposed ideology can be implemented in four phases to achieve security in unsecured channel, in addition this elevates the motivation of modulation in more descent way.

Encryption phase

In this phase the data to be sent through the channel undergoes archetypal encryption by using the encryption algorithm proposed [section 3].

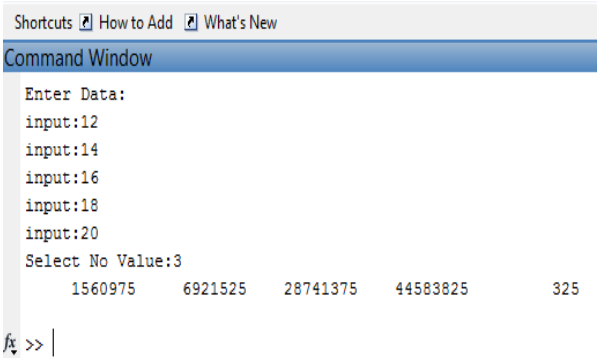


Figure-2. Modulation identifier algorithm.

The outcome of this archetypal algorithm is converted to binary form and saved in a file at the sender side as shown in Figure-2.

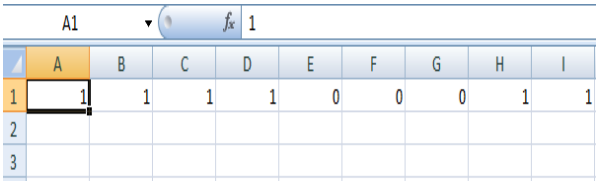


Figure-3. Encrypted data in binary form.

The bit size of the data converted is saved in file for decryption purpose further. Bit size is also converted into binary form to transmit it through network by performing modulation.

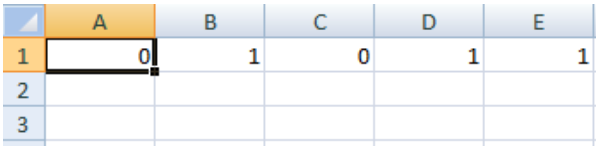


Figure-4. Bit size in binary form.

Modulation and demodulation phase

The corollary of encryption phase is treated as input for phase-2 i.e., modulation where security of the data is upgraded by varying some properties of periodic waveforms (carrier signals).

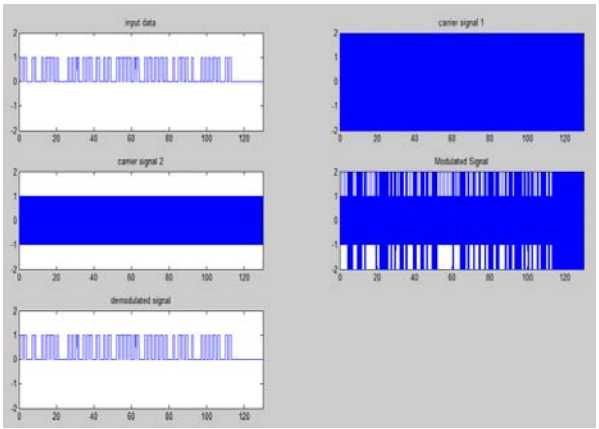


Figure-5. Results before and after modulation.

Resultant files of encryption phase are given as inputs to modulation. Two carrier signals are considered through which input is scrambled with. Modulated signal is transferred through the network by the transmitter.

Receiver after receiving the signal process the signal to demodulator, where demodulator demodulates the signal and gives the original input signal.

Decryption phase

The signal that is obtained after demodulation is then converted to binary form and saved in file. Data that is in binary format is converted to decimal form by using the bit size which is saved in encryption phase and transmitted to receiver. Data obtained after conversion

undergoes typical decryption algorithm proposed [section 3].

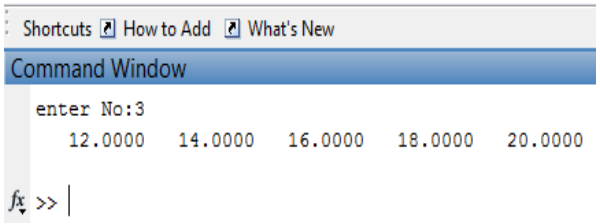


Figure-6. Result after decryption.

The outcome finally will be the original text we intended to send from source to destination.

6. CONCLUSIONS

The proposed work of the paper elevates a new approach of security along with modulation. The slant framed can be employed in unsecured channels which guarantee secure communication. Furthermore it ensures modulation of already well-Encrypted data which is secure. Enactment of this work promises the up gradation of security level of the data transferred through communication channel and effective adoption of modulation. This system ensures secure adoption of modulation in an unsecured network channel more efficiently.

REFERENCES

P. Polychronidou. 2011. Department of Accountancy. A non linear transform of Riesz product and an application in Encryption/ decryption. Kavala Institute of Technology, AgiosLoukas, 65404, Kavala, Greece. Published online: 29 May.

Johnson C. R. and Horn R. A. 1985. Matrix Analysis. Cambridge University Press, New York, USA.

Atreas N. D. and Polychronidou P. 2008. A class of sparse invertible matrices and their use for non-linear prediction of nearly periodic time series with fixed period. Numerical Functional Analysis and Optimization. Vol. 29(1), pp. 66–87.

Bhatt G., Kraus L., Walters L. and Weber E. 2006. On hiding messages in the oversampled Fourier coefficients. J. Math. Anal. Appl. Vol. 320, pp. 492–498.

Atreas N. D., Karanikas C. and Polychronidou P. 2008. A class of Sparse Unimodular matrices generating Multiresolution and Sampling Analysis for data of any length. SIAM Journal on Matrix Analysis and Applications, Vol. 30(1), pp. 312–323.

V. Raghunathan, C. Schurgers, S. Park, and M. Srivastava. 2002. Energy-Aware wireless microsensor networks. IEEE Signal Processing Magazine. Vol. 19, pp. 40–50, March.

Bauer L. F. 2007. Decrypted Secrets. 4th edition, Springer-Verlag Berlin Heidelberg.

C. H. Liu and H. H. Asada. 2002. A source coding and modulation method for power saving and interference reduction in DSCDMA sensor network systems. In: Proceeding American Control Conference. Vol. 4, pp. 3003-3008, May.

Goldreich O. 2001. Foundations of Encryption/ decryption: Basic Tools. Cambridge University Press, New York, USA.

Miotke J. R. and Rebollo-Neira L. 2004. Oversampling of Fourier coefficients for hiding messages. Appl. Comput. Harmon. Anal. Vol. 16(3), pp. 203-207.

Vaudenay S. 2006. A Classical Introduction to Encryption/ decryption. Springer Science and Business Media, New York, USA.

Juhana Yrjölä. 2005. Energy-Efficient Communication Protocol for Wireless Microsensor Networks, T-79.194 Seminar on theoretical computer science 2005 Algorithmics of sensor networks.

Estrin, D. Girod, L. Pottie, G.Srivastava, M. 2001. Instrumenting the world with wireless sensor networks. Proceedings (ICASSP '01) IEEE International Conference on Acoustics, Speech, and Signal Processing. Volume: 4, pp: 2033-2036.

Patil, H. K., and Szygenda, S. A. 2012. Security for wireless sensor networks using identity-based cryptography. CRC Press.

Prasad, B. K. V., Kumar, P. S., Charles, B. S., Madhu, T., and Ravi, S. 2014. Testing and reconfiguring the application based modulation suited for cognitive radio. In: Electronics and Communication Systems (ICECS). International Conference on. pp. 1-5. IEEE.

M. J. Handy, M. Haase, and D. Timmermann. 2002. Low energy adaptive clustering hierarchy with deterministic cluster-head selection. 4th International Workshop on Mobile and Wireless Communications Network. pp. 368-372.

Archana Bharathidasan, Vijay Anand Sai Ponduru. 2003. Sensor Networks: An Overview. IEEE Potentials, April-May. Volume: 22, Issue: 2, pp: 20- 23.

Ameer Ahmed Abbasi and Mohamed Younis. 2007. A survey on clustering algorithms for wireless sensor networks" Computer Communications, Volume 30, Issues 14-15, 15 October. pp. 2826-2841.

Wendi B. Heinzelman *et al*. 2002. An Application-Specific Protocol Architecture for Wireless Micro

sensorNetworks. IEEE transactions on wireless communications. vol. 1, no. 4, October.

C. Schurgers, O. Aberthorne, and M. B. Srivastava. 2001. Modulation scaling for energy aware communication systems. Proceeding, IEEE ISLPED. pp. 96-99, August.