Fully Secured Adhoc Wireless Network by using on Demand Half Full Weighing Matrices

S C Dutta
Assistant Professor
Department of Computer Science and Engineering
BIT Sindri,
Dhanbad-828123

Sudha Singh
Professor
Department of Computer Science and Engineering
MGM college of Engg. and Technology, Kamothe, Navi Mumbai-410209

D K Singh
Director
BIT Sindri, Dhanbad-828123

Abstract

An ad hoc wireless network is a collection of nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. Providing security support for such network is a challenging task. Masquerading, eavesdropping, resource consumption, interference and jamming are some of the major threats to such network. The scheme proposed in this paper gives a general framework to solve the security threats by designing on demand Half-full weighing matrix based cryptography scheme (ODHFWMBCS). It provides almost complete secure communication. ODHFWMBCS is a combination of code containing node identity and public key cryptography. For code, on demand half full weighing matrix have been constructed. The proposed scheme ODHFWMBCS gives a new direction towards more effective and efficient security design for ad hoc wireless networks.

Keywords: Adhoc wireless network, Public key cryptography, DES, RSA algorithm, Coding theory, Hadamard matrix, Sylvester Hadamard matrix, weighing matrix

I. INTRODUCTION

An adhoc wireless network is a wireless network comprised of mobile computing devices that use wireless transmission for communication, having no fixed infrastructure [8]. These network find application in several areas like military communication, emergency situations that need quick deployment of a network, hybrid wireless network etc. Security is the major concern in rapid development of such wireless communication. To provide security, the most widely used encryption scheme is based on the Data Encryption Standard (DES) [10] adopted in 1977 by the National Institute of Standards and Technology. The concept of the public key cryptography scheme was put forth by Diffie and Hellman [2] and the first realization of the public key cryptography was proposed by Rivest, Shamir and Adleman in 1978 [9].

At the simplest, the aim of cryptography is to maintain confidentiality of information transmitted over an insecure channel. The model is illustrated in following figure.

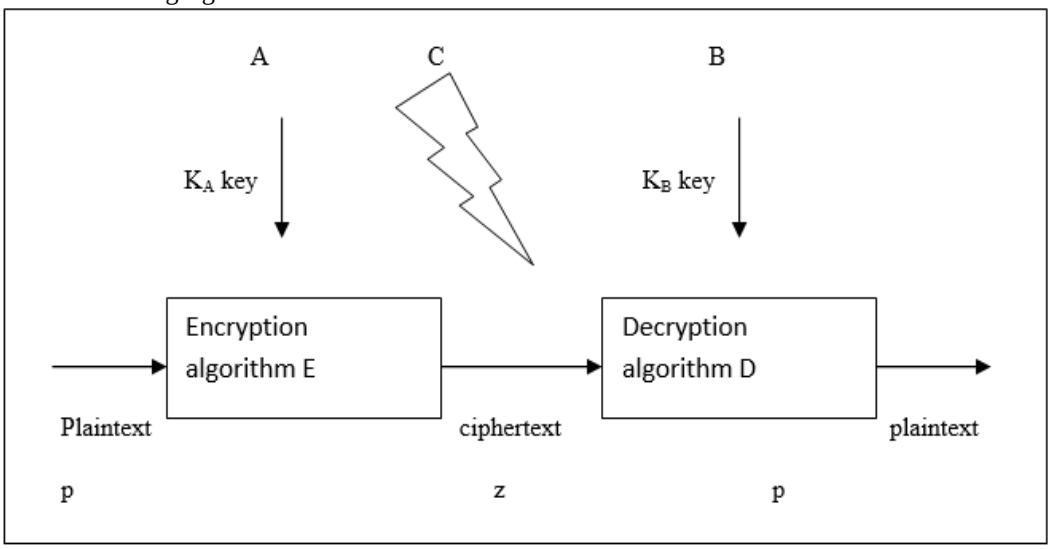

Fig. 1: Model of transmission over an insecure channel

A wants to send a message to B over a channel which is not secure, which only B is entitled to read,. An eavesdropper C may try to intercept the message and read or modify it. To avoid this, A and B agree to use a cryptographic system or cryptosystem, which consists of encryption and decryption algorithms. If message are to be sent frequently, it is practical to reuse the algorithms, but incorporate secret material, which can be changed at regular intervals.

A encrypts the message (plaintext p) using the encryption algorithm E with her key K_A and transmits the ciphertext $z=E(p, K_A)$ to B. B uses the decryption algorithm D with his key K_B to recover the message $p = D(z, K_B)$ of necessity, the encryption algorithm must be an invertible function, whatever message and keys are used, that is, $D(E(p, K_A),K_B)=p$ for all p, K_A,K_B.

Cryptosystems are of two main types, private key or symmetric systems, where the parties know each other and have disclosed information about their private keys, and public key or asymmetric systems, where it is not necessary that the parties know each other and they each have two keys obtained through a trusted authority, a public key published by the authority, and a private key they do not disclose to anyone. The best-known private key systems are DES (Data Encryption Standard) and its successor Rijndael, the AES competition winner. These algorithms are suited to fast high volume data transmissions. The best known public key system is RSA, which is slower but does not require the parties to exchange key information, and is suitable for key distribution and digital signature schemes. An encyclopedic coverage of cryptography in general appears in [10].

RSA algorithm[9] was discovered by a group at MIT in 1978. Their method is

- Choose two prime numbers p and q (typically greater than 10^{100}).
- Compute n = p x q and $\varphi(n) = (p-1) \times (q-1)$.
- Choose a number relatively prime to $\varphi(n)$ and call it e.
- Find d such that $e \times d \equiv 1 \bmod \varphi(n)$

Now divide the plain text into blocks of k(where k is the largest integer for which $2^k<n$) bits so that each plaintext P falls in the interval $0 \le P < n$. To encrypt a message P, compute $C = P^e \bmod n$. To decrypt C, compute $P = C^d \bmod n$. We can see the example in 9.2 section of chapter 9 in [10].

The RSA algorithm robustness is ensured by the complexity of large number factorization. RSA is too slow for actually encrypting large volume of data. Different weaknesses of this algorithm could be observed and many attacks against it are developed successfully.

Coding theory is an area of science lying in the intersection of Computer Science, Electronics and telecommunication engineering and Mathematics. The area emerged in the 1940s from the study of methods to transmit information reliably over noisy channels of communication. It is concerned with transmitting data across noisy channels and recovering message. In the seventy years since its conception, coding theory has grown into an extensive body of results, methods and applications. It draws extensively from methods in algebra and probability, and sees applications in theoretical computer science and cryptography as well as its original motivations, namely, storage and communication of information.

A Hadamard matrix is an n x n matrix M with entries from ± 1 such that $MM^T = nI_n$, where I_n is the n x n identity matrix. In other words, a Hadamard matrix is a square matrix M with entries from {1,-1}, for which the inner product of any pair of distinct rows is 0. A Hadamard matrix immediately leads to an error correcting code where the rows of M are the code words. This leads to a codeword over the alphabet A = { +1, -1}. The Hadamard codes maintain a constant distance rate. But, their message rate approaches zero very quickly[4].

Hadamard matrices have exerted a fascination over us for the past one-and-a-half centuries.

In daily life, the practical use of Hadamard matrices is constant and largely invisible. The Walsh-Hadamard Transform is in common use as a fast discrete transform. Error correcting codes(Reed-Muler codes) used in early satellite transmissions-for example, in 1972 Mariner mission to mars and recent flybys of the outer planets in the solar system-are based on Hadamard matrices. Modern CDMA cell phones use Hadamard matrices(Walsh covers) to modulate transmission on the uplink and minimize interference with other transmissions to the base station. New applications are everywhere about us, in pattern recognition, neuroscience, optical communication and information hiding, for example. Despite this, there is no uniform technique for constructing all the known Hadamard matrices.

Our curiosity and ingenuity does not stop at square matrices with entries from {+1,-1}.Hadamard matrices have been extended and generalized, to non-binary alphabets and higher dimensional arrays, and their desirable properties adapted for multilevel and multiphase applications in signal processing, coding and cryptography[4,5,6,7,13].

Elementary constructions of Hadamard matrices easily follow from its definitions: Let h be a Hadamard matrix of order n, so by definition it is invertible over Q, with $H^{-1} = n^{-1}H^T$. Set $H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Then

1) the negation –H of H is a Hadamard matrix;
2) the transpose H^T of H is a Hadamard matrix;
3) if H' is a Hadamard matrix of order n', the tensor product H' ⊗ H is a Hadamard matrix of order n'n;
4) for $t \ge 1, (\otimes^t H_1) \otimes H$ is a Hadamard matrix of order $2^t n$.

Sylvester Hadamard matrices: The earliest known, and still by far the most significant, family of hadamard matrices are those of order 2^t for $t \ge 1$, due to Sylvester. They are constructed by iterating the tensor product of H_1 with itself. These matrices are all symmetric.

Example:

$$H_1 \otimes H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

We can see the use of Hadamard matrices in design of experiments, Hadamard transform, spectroscopy, object recognition, for coding of digital signals, digital logic design, pattern recognition, data compression, magnetic resonance imaging, neuroscience and quantum computing, digital and satellite communication and is commonplace globally in CDMA mobile phones, but is an emergent techniques in automated learning, ultrasonic, optical communication and information hiding [4,5,6,7,13].

Weighing matrix: A weighing matrix W of order n with weight w is an $n \times n$ $(0,1,-1)$-matrix such that $WW^t = wI$, where W^t stands for transpose of W. A weighing matrix is called regular if its row and column sums are equal, and quasisymmetric if its pattern of zeros is symmetric.

Two weighing matrices W_1=[m_{ij}] and W_2=[n_{ij}], will be called complementary if $\begin{cases} m_{ij} = 0 \implies n_{ij} \neq 0 \\ n_{ij} = 0 \implies m_{ij} \neq 0 \end{cases}$

Recently weighing matrices have been found much beneficial to engineers working with satellite and digital communications. They have been found to have many similarities with perfect ternary arrays, and these arrays have been implemented in our digital communications.

II. CONSTRUCTION OF ON DEMAND HALF-FULL WEIGHING MATRIX

The construction of weighing matrix from Hadamard matrix[11] is given below

If $H = \begin{bmatrix} H_1 & H_2 \\ H_3 & H_4 \end{bmatrix}$ is a Hadamard matrix, then $W_{(n/2)} = \begin{bmatrix} H_1 + H_2 & H_1 - H_2 \\ H_3 + H_4 & H_3 - H_4 \end{bmatrix}$ will be a weighing matrix, where n is the order of H.

For standard proof we can see singh et. al.[12]. An immediate consequence of the theorem is that Hadamard matrix conjecture implies the Half-full weighing matrix conjecture. Craigen [1] remarked that half full conjecture has been confirmed for $4n \leq 212$. Theorem I of paper[12] confirms the conjecture for all values of n with $4n \leq 1000$ except for 4n=668,716,764 and 892, as Hadamard matrices of these orders are unknown (vide Horadam [4], page 25).

Let "+" denote 1 and "–" denote -1 .Then we can easily construct half full weighing matrix from weighing matrix as illustrated below

Illustration: If $H = \begin{bmatrix} H_1 & H_2 \\ H_3 & H_4 \end{bmatrix} =$

$$\begin{bmatrix} + & + & + & + & + & + & + & + \\ + & - & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & - & + & - & - & + & - & + \\ + & + & - & - & - & - & + & + \\ + & - & - & + & - & + & + & - \end{bmatrix},$$

Where + denote 1 and - denote -1, then

$$W = \begin{bmatrix} H_1 + H_2 & H_1 - H_2 \\ H_3 + H_4 & H_3 - H_4 \end{bmatrix} = \begin{bmatrix} + & + & + & + & 0 & 0 & 0 & 0 \\ + & - & + & - & 0 & 0 & 0 & 0 \\ + & + & - & - & 0 & 0 & 0 & 0 \\ + & - & - & + & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & + & + & + & + \\ 0 & 0 & 0 & 0 & + & - & + & - \\ 0 & 0 & 0 & 0 & + & + & - & - \\ 0 & 0 & 0 & 0 & + & - & - & + \end{bmatrix}$$

It is interesting to note that W will be Half-full weighing matrix. This property of W will open huge area of its applications. In adhoc wireless network most of the attacks are passive, masquerade and denial of service. In half-full weighing matrices, half of the elements are zero. Using signal with such a code almost removes passive type of attack and minimizes attacks like masquerade and denial of service. In above example W is a weighing matrix of order 8. For more secure communication we have to take n as a large number. If we take large value of n, then n/2 elements in W will be 0. It simply means there will be no signal value in those moments. It will nullify the study of eavesdroppers. And this is our aim! Of course! This will work great for small messages. In case of emergency and in adhoc wireless network, more than 90% messages are small.

III. METHOD OF USING ON DEMAND HALF-FULL WEIGHING MATRIX AS A CODE

Suppose in a case, we have to use adhoc wireless network. Then we know that in this case maximum n number of people are going to involve. According to the demand we will make half full weighing matrix with order n. We will make nodeID with the rows and provide this nodeID to the persons involved or going to involve in future.

So, we can say that proposed scheme is based on coding theory. Each node is assigned a code, which is a sequence of numbers with following properties:

1) Each sequence is made of n elements, where n is the number of nodes.
2) The inner product of two equal sequences is unique and is equal to n/2.
   [+1 +1 -1 -1 0 0 0 0] • [+1 +1 -1 -1 0 0 0 0] = 1 + 1 + 1 + 1 = 4 (which is equal to n/2)
3) The inner product of two different sequences is unique and is equal to 0.
   [+1 -1 +1 -1 0 0 0 0] • [+1 +1 -1 -1 0 0 0 0] = 1 -1 - 1 +1 = 0 (which is equal to 0)

If a node needs to send a 0 bit, it encodes it as -1;if it needs to send a 1 bit, it encodes it as +1. When a node is idle, it sends no signal, which is interpreted as a 0.

Let us assume we have n nodes in ad hoc wireless network. Let the code assigned to the first node be C1, to the second node be C2, and so on. We suppose that the data from node 1 is D1, from node 2 are D2, and so on.

In such network, it is not always possible that all nodes will send data simultaneously. Also all nodes are connected through each other.

Any node i can get the data by multiplying 2/n to the result given below:

$$\sum_{j=1}^{n} C_i * (C_j * D_j) = \left(\frac{n}{2}\right) * D_i$$

IV. ENHANCED RSA ALGORITHM FOR ADHOC WIRELESS NETWORK

Enhanced RSA method[3] is given below:

1) Select two very big prime numbers p and q.
2) Compute n = p x q and φ (n) = (p-1) x (q-1).
3) Public key component e(e<(φ (n)/10)) is randomly generated and prime to φ (n). Also e should not belongs to the set {3,5,7}. Conditions on e are applied to maintain the algorithm speed because we are working with keys containing large number of bits.
4) Find d such that e x d ≡ 1 mod φ (n)
5) In each block, different encryption key is used.
   $C_e = M^e \bmod n$; $C_e = M^e\, C_{e-1} \bmod n$, e≥7, and for each encryption key there is a different decryption key.
   $M_d = C^e \bmod n$; $M_d = C^e\, M_{d-1} \bmod n$.

Encryption and decryption should be done iteratively to avoid computational errors. Algorithm should compute iteratively the encrypted message to avoid computational errors caused by large numbers; $C_e = M^e \bmod n = (M.C_{e-1}) \bmod n$, where with various conditions on e. These conditions are required to improve the computational speed and security of RSA in adhoc wireless network. There should be often change in the encryption key for each input block to increase the robustness of the algorithm.

Algorithm for encryption part of enhanced RSA consists of four parts: Primary Number generation, Block Division, Key Generation and Encryption

1) Start
   ----------Prime number generation----------
2) Generate a random number p (512 bits)
3) Check if p is not a prime then go to step 2
4) Generate a random number q (512 bits)
5) Check if q is not a prime then go to step 4
6) Check if q = p then go to step 4
7) Generate n= p*q (1024 bits)
8) Generate phi = (p-1)*(q-1) (1024 bits)
   ---------Block division----------
9) Receive plain text from client socket program, t1

10) Convert it into bytes and store it into a byte array b1
11) Take Temporary variable temp to hold the previously generated cipher (1024 bits)
12) Initialize the counter i =0
13) If i >=b1.length then goto step 23
    ----------Key generation----------
14) Generate public key e (1024 bits) such that gcd(e,phi)=1 and 7< e < phi/10
15) Generate private key d (1024 bits) using d.e ≡ 1(mod phi)
16) Store e and d in different arrays
    ----------Encryption----------
17) If i=0 then cipher = m^e (mod n)
18) else cipher = m^e. C_{e-1}(mod n)
19) Store cipher into temp i.e. temp=cipher
20) return cipher to client socket
21) Increment counter i
22) Goto step 13
23) stop

Similarly decryption can be done.

V. FRAMEWORK FOR AN ON DEMAND HALF-FULL WEIGHING MATRIX BASED CRYPTOGRAPHY SCHEME AND TESTING

We suppose that all nodes are homogeneous and have almost equal processing power. For code, we are constructing on demand half full weighing matrix. For public key cryptography, enhanced RSA algorithm have been used. Any frame of ODHFWMBCS will have the five fields-identifier, encrypted data or cipher text, encrypted key with enhanced RSA, RSA private key and code. If data is large then we have to fragment it. Identifier is used to identify the data. Primary level of data security is provided by encrypting the data with symmetric key K, most probably using DES algorithm. This symmetric key will be included in the frame but in encrypted form. Key will be encrypted by enhanced RSA algorithm to provide 2nd level of security. We are providing 3rd and highest level of security in the form of code which is unique to each and every node. This unique code is a row of on demand half full weighing matrix with above mentioned features.

Identifier	*Encrypted data*	*Encrypted key with enhanced RSA*	*RSA private key*	*Code*
To identify the fragmented part	*Data will be encrypted by symmetric key K (It gives 1st level of security)*	*K will be encrypted by key (e_1,n) (It gives 2nd level of security)*	*RSA private key (d_1,n)*	*It contains the code C_i as a sequence of bits (It gives 3rd and highest level of security)*

The simulation of ODHFWMBCS has been done over 500 different scenarios. During testing, we observe that

1) Any node may lose secure connection with any node due to mobility but that node will be on network and can gain the secure connection back in any moment.

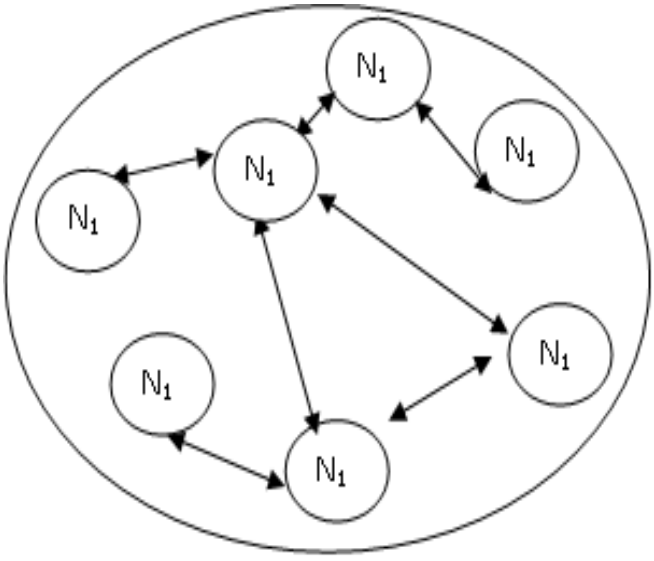

Fig. 2: An example of adhoc wireless network

2) Security key for connection is there with every node, so any other malicious node cannot get connected on this MANET.
3) If they have to send short messages they will use proposed RSA algorithm. Every node knows about the public key and private key can be sent through blocks. One case[3] for short message is given below (for long message see[3]):

Suppose message is "am". Every node know that what is n, e.g. 187.

Table – 1
Results of an example of proposed RSA algorithm.

Block No.	*E*	*Message*	*ASCII*	*C= M^e(mod n)*	*D*	*M=C^d(mod n)*	*Message*
1	*13*	*A*	*1*	*1*	*37*	*1*	*A*
2	*11*	*M*	*13*	*123*	*131*	*13*	*M*

4) Due to the conditions applied on φ (n), time required for computation is as low as multiplying two array of numbers means within a fraction of second. Encryption and decryption both are fast.
5) We can use different RSA keys for different message blocks for better security. Since speed is good we can use the key with 2048 bits for better security.
6) We assume that our message is in the form of binary digits or *bits*, strings of 0 or 1. We have to transmit these bits along a channel in which errors occur randomly.
7) The Hamming distance between two words (of the same size) is the number of differences between the corresponding bits. The minimum Hamming distance(d) is the smallest Hamming distance between all possible pairs in a set of words. A code word with minimum hamming distance d can detect d-1 errors and can correct (d-1)/2 errors.
8) Hence above ODHFWMBCS code can able to detect ((n/4)-1) errors and can able to correct (n-4)/8 errors.

VI. RESULT OF THE ON DEMAND HALF-FULL WEIGHING MATRIX BASED CRYPTOGRAPHY SCHEME

Features of the above scheme in different types of network are tabulated below:

Table – 2
Result 1.

Types of Network	*Key distributing center*	*Features*	*Weaknesses*
Adhoc wireless network (with fewer nodes)	*Pre-distributed*	*Security, Scalability, robustness, synchronization, transparency,better throughput, power control, minimize access delay etc*	*Limited energy resources, Information disclosure*
Wireless sensor network	*Base station/center node*	*Security, Scalability, robustness, better throughput, minimize access delay etc*	*Limited energy resources, Host impersonation/Information disclosure*
Wireless mesh network	*Pre-distributed/center node*	*Highly secure, Scalability, robustness, synchronization, transparency,better throughput, power control, minimize access delay etc*	*Limited energy resources, Information disclosure.*
Hybrid wireless network	*Base station*	*Minimized attack, Scalability, robustness, synchronization, transparency,better throughput, power control, minimize access delay etc*	*Limited energy resources, Host impersonation*
Cellular network	*Base station*	*Minimized attack, High throughput, Scalability, robustness, synchronization, transparency, power control, minimize access delay etc*	*Limited energy resources, Host impersonation*
Wireless network	*Base station/access point*	*Immune to attack, High throughput, Scalability, robustness, synchronization, transparency, power control, minimize access delay etc*	-

During different types of attack, working of above scheme on different types of network are tabulated below:

Table – 3
Result 2.

Attacks	*Adhoc wireless network*	*Wireless sensor network*	*Wireless mesh network*	*Hybrid wireless network*	*Cellular network*	*Wireless network*
Eavesdropping	√	√	√	√	√	√
Traffic analysis		√		√	√	√
Masquerade					√	√
Replay					√	√
Modification of messages		√				
Denial of service						
Jamming	√	√	√	√	√	√

During different types of attack, working of security services with above scheme on different types of network are tabulated below:

Table – 4
Result 3

Security Services	*Adhoc wireless network*	*Wireless sensor network*	*Wireless mesh network*	*Hybrid wireless network*	*Cellular network*	*Wireless network*
Authentication	√	√	√	√	√	√
Access control	√	√	√	√	√	√
Data confidentiality	√		√	√	√	√
Data integrity	√		√	√	√	√

Non repudiation	√	√	√	√	√	√

VII. CONCLUSION AND FUTURE WORK

The scheme proposed in this paper gives a general framework to solve the security threats by designing on demand Half-full weighing matrix based cryptography scheme (ODHFWMBCS). It provides almost complete secure communication. ODHFWMBCS is a combination of code containing node identity and public key cryptography. For code, we are constructing on demand half full weighing matrix. The proposed scheme ODHFWMBCS gives a new direction towards more effective and efficient security design for ad hoc wireless networks. We have used key length upto 1024 bits considering better security, computing speed and processor condition. Key length can be increased depending upon the conditions.

REFERENCES

[1] Craigen, R., "Weighing matrices and weighing designs in CRC Handbook of Combinatorial Designs **",** Eds: J. Dinitz and C Colburn, CRC Press, 1996**.**
[2] Difie W. and Hellman, M," Multiuser cryptographic techniques", IEEE transactions on Information theory, Nov. 1976.
[3] Dutta S. C., Singh Sudha and Singh D. K. "Enhancement of Mobile Adhoc Network security using Improved RSA algorithm", proceedings of Springer 2015 , vol 1, pp 1027 – 1036., 2015.
[4] Horadam, K.J., Hadamard matrices and their applications,Princeton University press, New Jersey,2007.
[5] Harwit, M. and N. J. A.Sloane, "Hadamard Transform Optics", Academic Press, New York, 1979.
[6] Hedayat A.S., N.J.A. Sloane and J. Stufken, "Orthogonal Arrays, Theory and Applications", Springer-Verlag, New York, 1999.
[7] Koukouvinos, C. and J. Seberry ,"Weighing matrices and their applications", Journal of Statistical planning and inference, Volume- 62, Issue-1, pp.91-101,1997.
[8] Muthy C S Ram and Manoj B S," Adhoc wireless network architecture and protocols", Pearson Education Inc, 20th edition, 2014.
[9] Rivest, R;Shamir, A and Adleman, L," A method for obtaining digital signatures and public key cryptosystems", Communications of the ACM, Vol.21(2), pp.120-126, 1978.
[10] Stallings W., "Cryptography and network security", Pearson education Inc., 4th edition, Tenth impression, 2011.
[11] Singh Sudha and Singh M. K.,"Simplified construction of weighing matrices from Hadamard matrices and its applications", Proceedings of IEEE International conference on Recent advances in IT, pp.889-891, 2012.
[12] Singh M. K., Singh Sudha and Singh S. K.,"On the construction of Weighing matrices",International Journal of Research and Reviews in Computer Science, Vol.1, No.4, pp.99-102, 2010.
[13] Sloane, N.J.A. and M. Harwit, Masks for Hadamard transform optics and weighing designs Applied Optics, Vol.15, pp.107-114,1976.