Study of the Effects of Noise on a New Model Based Encryption Mechanism with Time-Stamp and Acknowledgement Support in MANET & WSN Environment

A.V.N.Krishna
Pujyasri Madhanvanji College of Eng. & Tech.,
Hyderabad, India.
Email: hari_avn@rediffmail.com

Abstract

In this work the encryption mechanism in MANET & WSN is considered. One of the very important parameters with MANET & WSN is its low computing power availability in its real time environment. This study is based on a Mathematical model being used for encryption process, which consumes less power when compared to standard algorithms like 3 DES & RSA. The encrypted form of data during the transmission process will be subjected to errors due to some unavoidable noise sources. These errors can affect the integrity of message or data transfer. The effects of these errors are checked in the present study by modeling the error as a random number having Gaussian Probability Density Function. These errors are stored in a sub data base which can be made use of when corrupted sub key is received at the receiver's side.

Keywords: Gaussian Probability Density Function, Random Number Generators, Tridiogonal Matrix Algorithm, Cubic Spline Interpolation, Encryption Decryption Mechanism, Key & Sub key.

1. Introduction

Historically, encryption schemes were the first central area of interest in cryptography [1-9]. They deal with providing means to enable private communication over an insecure channel. A sender wishes to transmit information to a receiver over an insecure channel that is a channel which may be tapped by an adversary. Thus, the information to be communicated, which we call the plaintext, must be transformed (encrypted) to a cipher text, a form not legible by anybody other than the intended receiver. The latter must be given some way to decrypt the cipher text, i.e. retrieve the original message, while this must not be possible for an adversary. This is where keys come into play; the receiver is considered to have a key at his disposal, enabling him to recover the actual message, a fact that distinguishes him from any adversary. An encryption scheme consists of three algorithms: The encryption algorithm transforms plaintexts into cipher texts while the decryption algorithm converts cipher texts back into plaintexts. A third algorithm, called the key generator, creates pairs of keys: an encryption key, input to the encryption algorithm, and a related decryption key needed to decrypt. This work mainly deals with the algorithm which generates sub keys which provides sufficient strength to the encryption mechanism.

Partial differential equations to model multi scale phenomena are ubiquitous in industrial applications and their numerical solution is an outstanding challenge within the field of scientific computing [11-14]. The approach is to process the mathematical model at the level of the equations, before discretization, either removing non-essential small scales when possible, or exploiting special features of the small scales such as self-similarity or scale separation to formulate more tractable computational problems. Different types of data like static data, sequential data, and time stamped data & fully temporal data can be considered for theoretical study.

2. Literature Survey

Currently a lot of work is going on performance of MANET’s and WSN’s, where the study depends on TCP performance, routing algorithms. The underlying study with these things is lower power consumption of the mechanisms and security issues. In the work [20], the authors have made an attempt to justify the use of TCP variants for loss of packets due to random noise introduced in MANET’s and WSN’s. Another important parameter in MANET s & WSN s is its need for low power consumption of mechanisms. In their work [3], the authors proposed a mechanism which requires least power expended for each node to transmit just enough power to ensure reliable communication. Security to data transmitted is one more important parameter to be considered in MANET’s and WSN’s. In the work [15], the authors proposed a security mechanism where canned security solutions like IP Security may not work. In the work [9], the authors presented a mathematical model for generation of sub keys, which can be used for encryption & decryption purpose which provides security. The advantage with this model is it consumes less power when compared to conventional algorithms which makes it more suitable in MANET’s and WSN’s. The one more important issue to be considered in MANET’s and WSN’s, is the effect of noise on data transfer. In their work [14], the authors presented two analytical models to describe the noise levels in real network applications. In this work an attempt has been made to identify the effects of noise on security models [22], and means to overcome them by generating a random number generator based on Gaussian distribution.

3. Numerical Data Analysis

The fallowing are the steps to generate a numerical method for data analysis [16,1].

3.1. Discritization Methods

The numerical solution of data flow and other related process can begin when the laws governing these processes have been express differential equations. The individual differential equations that we shall encounter express a certain conservation principle. Each equation employs a certain quantity as its dependent variable and implies that there must be a balance among various factors that influence the variable. The numerical solution of a differential equation consists of a set of numbers from which the distribution of the dependent variable can be constructed. In this sense a numerical method is akin to a laboratory experiment in which a set of experimental readings enable us to establish the distribution of the measured quantity in the domain under investigation

Let us suppose that we decide to represent the variation of $\varnothing$ by a polynomial in x

$$\varnothing = a_0 + a_1x + a_2x^2 + \ldots\ldots\ldots\ldots a_nx^n \qquad \ldots\ldots\ldots\ldots(1)$$

And employ a numerical method to find the finite number of coefficients a1 , a2……….an. This will enable us to evaluate $\varnothing$, at any location x by substituting the value of x and the values of a's in the above equation.

3.2. Steady One Dimensional Data Flow

Steady state one-dimensional equation is given by $\partial./\partial x(k\ \partial T/\partial x)$ +s =0. 0 where k & s are constants. To derive the discretization equation we shall employ the grid point cluster. We focus attention on grid point P, which has grid points E, W as neighbors. For one dimensional problem under consideration we shall assume a unit thickness in y and z directions. Thus the volume of control volume is delx*1*1. Thus if we integrate the above equation over the control volume, we get

$$(K.\ \partial.T/.\partial X)_e - (K..\ \partial T/.\partial X)_w + .\int S.\ \partial.X = 0.0 \qquad \ldots\ldots\ldots\ldots\ldots(2)$$

If we evaluate the derivatives, $\partial T/\ \partial X$ in the above equation from piece wise linear profile , the resulting equation will be $K_e(T_e - T_p)/(\partial X)_e - K_w(T_p - T_w)/(\partial X)_w$ + S *del x=0.0 where S is average value of s over control volume. This leads to discretization equation

$$a_pT_p = a_eT_e + a_wT_w + b \text{ Where } a_e= K_e/\partial X_e \qquad \ldots\ldots\ldots\ldots\ldots (3)$$

$$a_w = K_w/dX_w \qquad \ldots\ldots\ldots\ldots\ldots (4)$$

$$a_p= a_e+a_w-s_p.delX \qquad \ldots\ldots\ldots\ldots\ldots (5)$$

$$b=s_e.delX \qquad \ldots\ldots\ldots\ldots\ldots (6)$$

3.3. Solution of Linear Algebraic Equations

The solution of the discritization equations for the one-dimensional situation can be obtained by the standard Gaussian elimination method. Because of the particularly simple form of equations, the elimination process leads to a delightfully convenient algorithm. For convenience in presenting the algorithm, it is necessary to use somewhat different nomenclature. Suppose the grid points are numbered 1,2,3…ni where 1 and ni denoting boundary points. The discritization equation can be written as

$$A_i\ T_i + B_iT_{i+1} + C_iT_{\ i-1} = D_i \qquad \ldots\ldots\ldots\ldots\ldots (6)$$

For i = 1,2,3………….n_i. Thus the data value T is related to neighboring data values $T_{\ i+1}$ and $T_{\ i-1}$. For the given problem C_1=0 and B_n=0; These conditions imply that T_1 is known in terms of T_2. The equation for i=2, is a relation between T_1, T_2 & T_3. But since T_1 can be expressed in terms of T_2, this relation reduces to a relation between T_2 and T_3. This process of substitution can be continued until T_{n-1} can be formally expressed as T_n. But since T_n is known we can obtain T_{n-1}.This enables us to begin back substitution process in which $T_{n-2}, T_{n-3} \ldots\ldots\ldots\ldots T_3, T_2$ can be obtained. For this Tridiogonal system, it is easy to modify the Gaussian elimination procedures to take advantage of zeros in the matrix of coefficients.

Referring to the Tridiogonal matrix of coefficients above, the system is put into a upper triangular form by computing new Ai.

$$A_i = A_i - (C_{i-1} / A_i) * B_i \text{ where } i = 2,3 \ldots\ldots\ldots\ldots\ldots n_i. \qquad \ldots\ldots\ldots\ldots\ldots (7)$$

$$D_i = D_i - (C_{i-1} / A_i) * D_i \qquad \ldots\ldots\ldots\ldots\ldots (8)$$

Then computing the unknowns from back substitution

$$T_n = D_n / A_n \qquad \ldots\ldots\ldots\ldots\ldots (9)$$

Then, $$T_n = D_k - A_k * T_{k+1} / A_k,\ k= n_{i-1}, n_{i-2} \ldots 3,2,1 \qquad \ldots\ldots\ldots\ldots\ldots (10)$$

4. Mathematical Modeling of the Problem

The approach to time series analysis was the establishment of a mathematical model describing the observed system. Depending on the appropriation of the problem a linear or nonlinear model will be developed. This model can be useful to generate data at different times to map it with plain text to generate cipher text.

4.1. Linear Data Flow Problem

The initialization vector (IV) considered in the problem is When t=0, T (I) =Y (I) =300 where i=1,2,……..M.

Dividing the problem area into M number of points, and for simplicity by assuming data of the first and M_{th} grid points are considered to be known and constant. For the grid points 2, M-1, the coefficients can be represented by considering the conservation equation,

$$\alpha/\partial.x\,(T_{I+1}^{\;n+1} - T_I^{\;n+1}) + \alpha/\partial x\,(T_I^{\;n+1} - T_{I-1}^{\;n+1}) = (\partial x)/\partial t\,(T_I^{\;n+1} - T_I^{\;n}) \qquad \ldots..(11)$$

where T_I represents data value for the considered grid point for the preceding delt, $T_{I+1}^{\;n+1}$ & $T_I^{\;n+1}$ represents data values for the preceding and succeeding grid points for the current delt.

Considering α which is a key for the given model, the coefficients are obtained for each state (grid point) in terms of A(I) refers to data value of the corresponding grid point, C(I) and

B(I) refers to data values of preceding and succeeding grid points for the current delt, D(I) refers to data value of the considered grid point in the preceding delt.

$$A(I)= 1 + 2\,\alpha\,\text{delt}/(\text{delx})^{**}2 \quad \ldots\ldots\ldots\ldots..(12)$$

$$B(I)= -\alpha\,\text{delt}/(\text{delx})^{**}2 \quad \ldots\ldots\ldots\ldots..(13)$$

$$C(I)= -\,\alpha\,\text{delt}/(\text{delx})^{**}2 \quad \ldots\ldots\ldots\ldots..(14)$$

$$D(I)= T_I^{\,n} \quad \ldots\ldots\ldots\ldots..(15)$$

4.2. Procedure for Generating Data from Coefficients by Tridiogonal Method

These conditions imply that T_1 is known in terms of T_2. The equation for i=2, is a relation between T_1, T_2 & T_3. But since T_1 can be expressed in terms of T_2, this relation reduces to a relation between T_2 and T_3. This process of substitution can be continued until T_{n-1} can be formally expressed as T_n. But since T_n is known we can obtain T_{n-1}.This enables us to begin back substitution process in which T_{n-2},T_{n-3}…………T_3,T_2 can be obtained**.** This process is continued until further iterations cease to produce any significant change in the values of T’s. Finally the data distribution is obtained for all grid points for different times by considering a suitable α which is used as key.

5. Effect of Transmission Errors on Data Transfer

The encrypted form of data during the transmission process will be subjected to errors due to some noise sources. These errors can affect the integrity of message or data transfer. The effects of these errors are checked in the present study by modeling the error as a random number having Gaussian Probability Density Function (see Fig. 1(a) and 1(b)). The random number generator modeled is used to create values of the possible data errors. These errors are stored in a sub data base which can be made use of when corrupted sub key is received at the receiver’s side. Thus when the received message after decryption is showing any ambiguity in its meaning or any integrity variations because of noise, it can be checked using the sub data base developed by the random number generator model.

Algorithm of Random Generation Model

```
Subroutine random(x1, x2)
Common iseed
Pi=3.14
dum =1.0
ter=rand(dum)
term=abs(alog(ter))
term1= sqrt(2.0*term)
term2= 2*pi*rand(dum)
x1= term1*cos(term2)
x2= term1*sin(term2)
return end
```

Fig.1(a): *Algorithm of Random Generation Model*

Function to generate a uniform random number

```
function rand(dum)
Common iseed
Integer *4 iseed, idata, imax
Data = idata/127773
Imax= 2147483647
Ki= iseed/idata
Iseed= 16807( iseed-ki*idata)-ki*2836
If(iseed<0)
Iseed= iseed+imax
Rand= float(iseed)/float(imax)
Return End.
```

Fig.1(b): *Function to Generate a Uniform Random Number*

Sub data generated from the random model (see Fig. 2).

Data value(Sub key)	Iseed 70	Iseed 80	Iseed 90	Iseed 100	Iseed 110	Iseed 120
33	33	34	35	34	34	33
06	05	05	04	06	05	05
07	08	06	08	05	07	07
33	32	33	32	35	33	34
08	08	09	08	07	08	08
11	11	12	11	13	12	12
13	11	12	11	15	12	11
32	33	34	33	33	32	35
22	22	22	23	22	21	21
29	30	33	33	30	32	32
20	22	21	23	22	21	21
26	26	26	27	27	25	28
0	2	1	1	1	2	3
18	18	19	18	17	20	20
10	11	11	13	12	14	11
17	17	17	19	16	17	17
11	11	12	12	13	14	12
01	1	2	1	1	2	4
1	1	1	2	2	1	1

X-axis: Data Values
Y-axis: Grid Points

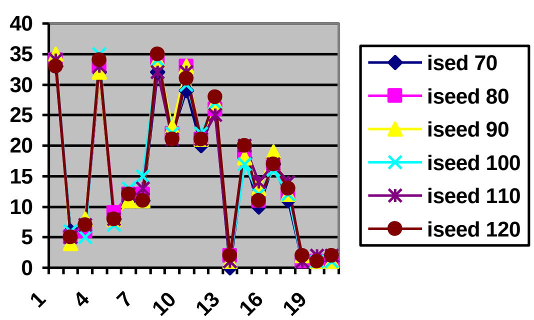

Fig. 2: Sub Data Generated from the Random Model

6. Results

By considering a suitable key α =4, del t= 2, delx =2 for a total time stamp of 6 units, Different data values obtained are For del t=2, time =2;

33 6 7 4 33 8 11 13 32 22 29 20 26 0 18 10 17 11 1 1;

For delt =2, time=4;

8 22 4 3 5 11 11 13 5 30 22 4 17 14 28 27 29 29 15 1
3 30 2 6 27 12 10 15 29 1 26 26 3 32 0 4 18 8 1 32

For delt =2, time=6;

33 6 7 4 33 8 11 13 32 22 29 20 26 0 18 10 17 11 1 1;
3 26 34 17 16 29 11 19 0 23 22 11 33 6 14 13 3 1 4 7;
3 10 21 23 5 33 9 18 0 20 31 17 15 18 6 14 0 9 31 1;

Thus by using the same key, by changing the time stamp values different sequences can be generated which are used as sub keys. These sub keys can be mapped to plain text to generate cipher text [14,16].

Encryption

Plain Text	**A**	**S**	**K**	**s**
Conversion to alpha numeric value	10	28	20	28
Sub key	33	6	7	4
Total	43	34	27	32
Mod 36	07	34	27	32
Cipher Text	07	Y	R	w

Decryption

Cipher Text	**07**	**Y**	**R**	**w**
Conversion to alpha numeric value	07	34	27	32
Add 36 if less than 9	43	34	27	32
Sub key	33	6	7	4
Subtract	10	28	20	28
Plain Text	A	s	K	s

7. Security Analysis

Analysis by Construction: In the given model, even though a single valued key is used, it also depends on time stamp. By changing the time stamp different values can be generated. By keeping the initialization vector constant, different values can be generated which provides good security against crypto analysis. Since the model involves not only key, time stamps but also data of past time stamps, it is relatively free from cipher text attack, known plain text & cipher text attacks. The given model is studied for its improved performance against noise with out compromising the security of the mechanism.

8. Conclusion & Future Work

This encryption mechanism uses an Initialization Vector, Time Stamp & Key to generate distributed sequences which are used as sub-keys. The model is studied for its improved strength against noise which is a unavoidable feature with MANET & WSN‘s. The model can also be studied for its strength against noise by using a non linear key.

References

[1] Hussein Al-Bahadili and Rami Jaradat, "Performance Evaluation of an OMPR Algorithm for Route Discovery in Noisy MANETs, International Journal of Computer Networks & Communications (IJCNC), Vol. 2, No. 1, January 2010.

[2] Hussein Al-Bahadili , Shakir M. Hussain , Ghassan Issa , and Khaled El-Zayyat : Performance Evaluation of the TSS Node Authentication Scheme in Noisy MANETs, International Journal of Network Security, Vol.12, No.3, PP.121{129, May 2011

[3] Hussein Al-Bahadili, Khalid Kaabneh: Analyzing the performance of probabilistic algorithm in noisy manets, International Journal of Wireless & Mobile Networks (IJWMN), Vol.2, No.3, August 2010

[4] Jorse Hortelano et al: "Testing applications in MANET environment through Emulation", EURASIP Journal of wireless communication and Networking, Vol 2009, ID 406974

[5] J.William stalling :Cryptography and network security (Pearson Education,ASIA1998)

[6] Krishna A.V.N., Vishnu Vardhan.B:Decision Support Systems in Improving the performance of rocket Missile systems, Giorgio Ranchi, Anno LXIII,n-5 Septembre-October 2008, pp607-615.

[7] Krishna A.V.N., S.N.N.Pandit: A new Algorithm in Network Security for data transmission, Acharya Nagarjuna International Journal of Mathematics and Information Technology, Vol: 1, No. 2, 2004 pp97-108

[8] Krishna A.V.N, S.N.N.Pandit, A.Vinaya Babu: A generalized scheme for data encryption technique using a randomized matrix key, Journal of Discrete Mathematical Sciences & Cryptography, Vol 10, No. 1, Feb 2007, pp73-81

[9] Krishna A.V.N., A.Vinaya Babu: A New mathematical model for encryption in network security., International journal for network security, NOV. 2010.

[10] Krishna A.V.N, A.Vinaya Babu: Pipeline Data Compression & Encryption Techniques in e-learning environment, Journal of Theoretical and Applied Information Technology, Vol 3, No.1, Jan 2007, pp37-43

[11] Krishna, A., Babu, A.. A New Non Linear, Time Stamped & Feed Back Model Based Encryption Mechanism With Acknowledgement Support. **International Journal Of Advancements In Technology**, North America, 1, Oct. 2010. Available At: Http://Ijict.Org/Index.Php/Ijoat/Article/View/Time-Stamped-And-Feedback-Model.

[12] Lester S. Hill, Cryptography in an Algebraic Alphabet, The American Mathematical Monthly 36, June-July 1929, pp306–312.

[13] Lester S. Hill, Concerning Certain Linear Transformation Apparatus of Cryptography, The American Mathematical Monthly 38, 1931, pp135–154.

[14] Madhavi W.Subbarao: " Dynamic power Conscious routing for MANETs", Journal of Research of the national Institute of standards & Technology, Vol 4, 1999.

[15] Nish Gorg, R.P.Mahapatra: " MANET Security issues", IJCSNS, Vol 9, No. 8, 2009.

[16] Pandit S.N.N (1963): Some quantitative combinatorial search problems. (Ph.D. Thesis).

[17] Phillip Rogaway : Nonce Based Symmetric Encryption, www.cs.ucdavis.edu/rogeway.

[18] Raja Ramanna Numerical methods 78-85(1990).

[19] R.S.Thore & D.B.Talange: Security of internet to pager E-mail messages (Internet for India, 1997IEEE Hyderabad section) pp.89-94.

[20] Shaminul Pamer, Kumar Monoj: "Input as Random loss on TCP performance in Mobile Adhoc Networks(IEEE 802.11), A Simulation based study", IJCSIT, Vol 7, No. 1, 2010.

[21] Suhas V. Patenkar Numerical Heat Transfer and Fluid Flow 11-75(1991).

[22] Xu Su, Rajendra Bopanna " On the impact of noise on MANET s", International cnference on Wireless Communications and Mobile Computing, 2007, PP 208-13.