Study of the Effects of Noise & Future Time Stamps on a New Model Based Encryption Mechanism

A. V. N. Krishna[1] and **P. V. Sarat Chand**[2]

Submitted in June 2010; Accepted in November 2010

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. Thus Security is an equal parameter in theses environments and equally important is its low computing power. This study is based on a Mathematical model [11] being used for encryption process, which consumes less power when compared to standard algorithms like 3 DES & RSA. This model generates a distributed sequence which is used as sub key. To generate sub key, variable time stamps are used. These time stamps are going to be generated by the same model. The model is also studied for handling errors in data transmission particularly in MANET/WSN environments.

KEYWORDS

Cubic spline interpolation, Encryption Decryption Mechanism, Gaussian probability density function, Key & Sub key, Random number generators, Time stamp and Nonce, Tridiogonal matrix algorithm.

1.0 INTRODUCTION

Historically, encryption schemes were the first central area of interest in cryptography[2-12]. 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 multiscale phenomena are ubiquitous in industrial applications and their numerical solution is an outstanding challenge within the field of scientific computing[11]. 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.

2.0 LITERATURE SURVEY

Currently a lot of work is going on performance of Manets (Mobile Adhoc Networks) and WSN(Wireless sensor Networks) [1], 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 [14], the authors have made an attempt to justify the use of TCP variants for loss of packets due to random noise introduced in MANETs and WSNs. Another important parameter in MANET s & WSN s is its need for low power consumption of mechanisms. In their work[5], 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 MANETs and WSNs. In the work [15], the authors proposed a security mechanism where canned security solutions like IP Security may not work. In the work[11], 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 MANETs and WSNs. The one more important issue to be considered in MANETs and WSNs, is the effect of noise on data transfer. In their work[22], 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[20],

[1] *Pujyasri Madhanvanji College of Engineering and Technology, Hyderabad, Andhra Pradesh, INDIA.*
[2] *Department of Computer Science, Indur Institute of Engineering and Technology, Andhra Pradesh, INDIA.*
[1] *hari_avn@rediffmail.com*

and means to overcome them by generating a random number generator based on Gaussian distribution.

3.0 NUMERICAL DATA ANALYSIS

The fallowing are the steps to generate a numerical method for data analysis[21].

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

$\varnothing = a_0 + a_1 x + a_2 x^2 + \ldots\ldots\ldots\ldots\ldots\ldots\ldots.. a_n x^n$

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 discretisation 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

$(K. \partial T/.\partial X)_e – (K.. \partial T/.\partial X)_w + .\int S. \partial.X = 0.0$ (eq. 1)

If we evaluate the derivatives $\partial T/ \partial X$ in the above equation from piece wise linear profile , the resulting equation will be

Ke(Te – Tp)/(∂X)e – Kw(Tp – Tw)/(∂X)w +
S *del x=0.0 (eq. 2)

where S is average value of s over control volume.

This leads to discretization equation

$a_p T_p = a_e T_e + a_w T_w + b$ (eq. 3)

Where $a_e = K_e/\partial X_e$
$a_w = K_w/dX_w$
$a_p = a_e + a_w - s_p.delX$
$b = s_e.delX$.

3.3 SOLUTION OF LINEAR ALGEBRAIC EQUATIONS

The solution of the discretisation 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 discretisation equation can be written as

$A_i T_i + B_i T_{i+1} + C_i T_{i-1} = D_i$

For I = 1,2,3…………ni. 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 $B_n=0$;

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

Ai = Ai – (Ci-1 /Ai)* Bi where i = 2,3………ni. (eq 4)
Di= Di – (Ci-1 /Ai) * Di (eq 5)

Then computing the unknowns from back substitution

Tn = Dn / An. (eq 6)

Then Tn = Dk – Ak * Tk+1 / Ak, k= ni-1, ni-2…3,2,1. (eq 7)

4.0 MATHEMATICAL MODEL

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 Mth 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,

$\alpha/\partial.x (T_{I+1}{}^{n+1} - T_I{}^{n+1}) + \alpha/ \partial x (T_I{}^{n+1} - T_{I-1}{}^{n+1}) =$
$(\partial x) /\partial t (T_I{}^{n+1} – T_I{}^{n})$ (eq.8)

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 α delt/(delx)**2. (eq. 9)
B(I)= -α delt/(delx)**2. (eq. 10)
C(I)= - α delt/(delx)**2. (eq. 11)

$D(I)= T_{I}^{n}$ (eq. 12)

4.2 PROCEDURE FOR GENERATING DATA FROM COEFFICIENTS BY TRIDIOGONAL METHOD

Using the coefficients of grid points, and by using the tridiogonal matrix algorithm, the data distribution is calculated. The grid points are numbered 1,2,3,…………M. with points 1 and M denoting extreme states.

The discretisation equation can be written as

Ai Ti + BiTi+1 +CiTi-1 = Di

For I = 1,2,3…M. Thus the data Ti is related to neighboring data values Ti+1 and Ti-1. For the given problem C1=0 and BM=0 as T1 & TM represent boundary states.

These conditions imply that T1 is known in terms of T2. The equation for I=2, is a relation between T1, T2 & T3. But since T1 can be expressed in terms of T2 , this relation reduces to a relation between T2 and T3. This process of substitution can be continued until TM-1 can be formally expressed as TM. But since TM is known we can obtain TM-1.This enables us to begin back substitution process in which TM-2, TM-3…T3, T2 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.

5.0 IDENTIFYING FUTURE TIME STAMPS FOR DATA GENERATION

In the given mathematical model[11], the data is calculated for different time stamps, which are fixed in nature. If variable time stamps are used, then the cryptoanalysis of the algorithm is more complex which increases the strength of the algorithm. To calculate variable time stamps the same model[11] can be used. The key remains the same with initial delt, delx also remains the same. Initial time stamp is considered.. Any random time stamp also being considered. By using the coefficients generated by the model, by using initial and intermediate time stamps, future time stamps are generated. These time stamps are considered in the model to generate sub key values.

6.0 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. The random number generator modeled is used to create values of the possible data errors. These errors are stored in a sub database 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.

By considering a suitable key α =4, del t= 2, delx =2 .

Initial time stamp =2, Intermediate time stamp=6;

Interpolated and Future time stamps generated by using the model are

3, 4.8.5.99, 7.2, 8.6, 10.2, 12.8.

Different data values obtained using these time stamps are

30 6 7 5 33 8 11 12 32 22 29 28 8 0 18 10 17 11 1 19;

7.0 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;

30 6 7 5 33 8 11 12 32 22 29 28 8 0 18 10 17 11 1 19;

For delt =2, time=4;

3 3 22 6 27 12 10 10 29 1 26 13 3 32 5 4 18 8 1 1

For delt =2, time=6;

9 7 2 5 5 30 9 18 0 2 31 17 15 6 6 14 0 8 31 22;

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 [13,15].

8.0 SECURITY ANALYSIS

Analysis by Construction: In the given model, a single valued key is used to generate interpolated & future time stamps which in turn are used to calculate sub key values. For variable time stamps, the model generates different sub key values which provide sufficient security against crypto analysis. Since the model involves not only key, but also interpolated & future 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

9.0 CONCLUSION & FUTURE WORK

This encryption mechanism uses a Initialization Vector, Interpolated & future Time Stamps & 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 using a non linear key can also be studied for its strength against noise.

REFERENCES

[1]. E. Jenefa JebaJothi , V. Kavitha and T. Kavitha Contention Based Routing in Mobile Ad Hoc Networks with Multiple Copies , Journal of computing, Volume 2, Issue 5, May 2010

[2]. Henry Baker and Fred Piper : Cipher systems(North wood books, London 1982).

[3]. H. Safa, O. Mirza, A load balancing energy efficient clustering algorithm for MANETs International journal of

communication systemsIssue ,Volume 23, Issue 4, pages 463–483, April 2010

[4]. I.Chien-Chiang: Efficient improvement to XTR and two padding schemes for probabilistic trapdoor one way function, 2005-12-05.

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

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

[7]. Krishna A.V.N.: A new algorithm in network security, International Conference Proc. Of CISTM-05, 24-26 July 2005, Gurgoan, India.

[8]. 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.

[9]. 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

[10]. 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

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

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

[13]. Mohammed F. Al-Hunaity, Salam A. Najim, Ibrahiem M. El-EmaryA comparative study between various protocols of MANET networks American Journal of Applied Sciences, Sept, 2007 .

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

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

[16]. P.K.Suri Kavita Taneja: Exploring Selfish Trends of Malicious Mobile Devices in MANET Journal of Telecommunications, Volume 2, Issue 2, May 2010

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

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

[19]. 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.

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

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

Table 1: Sub data generated from the random model

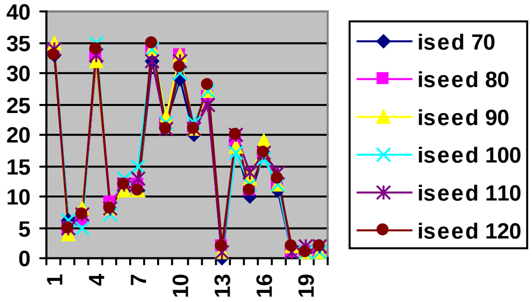

Figure 1: X- axis: Grid points
Y- axis: Data values over grid points

Continued on page no. 33